T.C.

ANTALYA BILIM UNIVERSITY

INSTITUTE OF POSTGRADUATE EDUCATION

CYBER SECURITY MASTER’S THESIS

NON-FUNGIBLE TOKENS (NFTS) AND THEIR SECURITY CHALLENGES

Yazeed Essam Khaled AL-THUNIBAT

DECEMBER 2022

ANTALYA

T.C.

ANTALYA BILIM UNIVERSITY

INSTITUTE OF POSTGRADUATE EDUCATION

CYBER SECURITY MASTER’S THESIS

NON-FUNGIBLE TOKENS (NFTS) AND THEIR SECURITY CHALLENGES

Yazeed Essam Khaled AL-THUNIBAT

DECEMBER 2022

ANTALYA

T.C.

ANTALYA BILIM UNIVERSITY

INSTITUTE OF POSTGRADE EDUCATION

NON-FUNGIBLE TOKENS (NFTS) AND THEIR SECURITY CHALLENGES

Yazeed Essam Khaled AL-THUNIBAT

This thesis was accepted by the jury (with unanimous vote/majority vote) on the date 17/01/2023 in CYBER SECURITY of CYBER SECURITY DEPARTMENT.

Asst. Prof. Asli BAY (Supervisor)

Dr. Onur KOÇAK

Prof. Dr. Cafer ÇALIŞKAN

Director of the Institute
Prof.Dr. İbrahim Sani MERT

Thesis Submission Date: / /202

DECLARATION

Msc Thesis of this study named “Non-Fungible Tokens (NFTs) and Their Security Challenges”, which I presented, I declare that scientific moral principles were followed in the preparation of this study, in case of benefiting from the works of others, reference is made in accordance with scientific norms, no falsification has been made in the data used, and that any part of this study is not presented as another academic study.

29 / 12 / 2022

Yazeed Essam Khaled AL-THUNIBAT

CONTENTS

ABSTRACT

NON-FUNGIBLE TOKENS (NFTS) AND THEIR SECURITY CHALLENGES

Yazeed Essam Khaled ALTHUNIBAT

Master Thesis in Cybersecurity

Supervisor: Asst. Prof. Aslı BAY

December 2022; 47 pages

The Non-Fungible Token (NFT) market has been exploding in the past years. The notion of NFT originated with Ethereum's token standard, which aimed to differentiate each token using distinguishing signals. Tokens of this type can be associated with virtual or digital properties to serve as unique identifiers. Using NFTs Non-Fungible Token (NFT) is a new technology gaining traction in the Blockchain industry.

In this article, we examine state-of the art NFT systems that have the potential to reshape the market for digital virtual assets. We will assess the security of existing NFT systems and expand on the opportunities and prospective uses for the NFT idea. Finally, we discuss existing research challenges that must be overcome before mass-market penetration may occur. We hope that this paper provides an up-to-date analysis and summary of existing and proposed solutions and projects, making it easier for newcomers to stay current.

KEYWORDS: Blockchain, Metaverse, Non-Fungible Token, NFTs, Security

COMMITTEE: Asst. Prof. Asli BAY

Dr. Onur KOÇAK

Prof. Dr. Cafer ÇALIŞKAN

ÖZET

İŞLEVSİZ BELİRTEÇLER (NFTS) VE GÜVENLİK ZORLUKLARI

Yazeed Essam Khaled ALTHUNIBAT

Yüksek Lisans Siber Güvenlik

Danışman: Asst. Prof. Aslı BAY

Aralık 2022; 47 sayfa

Fonksuz Belirteç (NFT) pazarı son yıllarda patlama yapıyor. NFT'nin nosyonu Ethereum'un belirteç standardıyla ortaya çıkmıştır ve bu durum, her belirteci ayırt edici sinyaller kullanarak ayırt etmeyi amaçlamaktadır. Bu tipteki belirteçler, benzersiz tanımlayıcılar olarak hizmet vermek için sanal veya dijital özelliklerle ilişkilendirilebilir. NFTS Non-Fungible Token (NFT) kullanmak, Blockchain endüstrisinde yeni bir teknoloji kazanıyor.

Bu makalede, dijital sanal varlıklar için pazarı yeniden şekillendirme potansiyeline sahip son teknoloji ürünü NFT sistemlerini inceliyoruz. Mevcut NFT sistemlerinin güvenliğini değerlendirecek ve NFT fikri için fırsatları ve olası kullanımları genişleteceğiz. Son olarak, kitle pazara giriş gerçekleşmeden önce aşılması gereken mevcut araştırma zorluklarını ele alıyoruz. Bu incelemede, mevcut ve önerilen çözüm ve projelerin güncel bir analizi ve özeti sağlanarak, yeni gelenlerin güncel kalmasını kolaylaştırılmasını umuyoruz.

Anahtar Sözcükler: Blockchain, Metaverse, Özel Eşdeğer Öğe, NFTler, Güvenlik

JÜRİ: Asst. Prof. Asli BAY

Dr. Onur KOÇAK

Prof. Dr. Cafer ÇALIŞKAN

ABBREVIATIONS

AR	**:** Augmented Reality
NFT	**:** Non-Fungible Token
POS	**:** Proof of Stake
POW	**:** Proof of Work
VR	**:** Virtual Reality
XR	**:** Cross Reality

LIST OF TABLES

TABLE OF FIGURE

PREFACE

This Master of Cyber Security dissertation deals with the security challenges of NFTs' as part of this study, a detailed and diverse research concerning the subject was analyzed. I would like to thank my supervisor, Asst. Prof. for guiding me and for sharing their knowledge throughout this study. I would also like to thank my family and friends for their support.

29/12/2022

Yazeed Essam Khaled Althunibat

1. INTRODUCTION

1.1 Blockchain

A decentralized and distributed database, known as a Blockchain, allows multiple parties to record and verify transactions securely and transparently without relying on a central authority. It consists of a network of computers, also called nodes, that each maintain a copy of a shared digital ledger that records all the transactions that have occurred on the network (Houben & Snyers, 2018).

The ledger is divided into blocks, each of which holds a record of multiple transactions. These nodes connect with one another in a chain through the use of cryptographic techniques, creating a secure and unbroken chain of blocks starting with the first block, known as the "genesis block." These links between blocks ensure the integrity and security of the ledger."

Blockchain is decentralized in the sense that it is administered by a peer-to-peer network of nodes, which makes it possible for it to be used as publicly distributed ledger in the future. A Blockchain is a list of record that is immutable and is constantly growing and connected to one another via cryptography. It all started in 1991, when Stuart Haber and W. Scott Storyette came up with the idea of a cryptographically secure chain of blocks that would prevent anyone from altering the timestamps on documents. This was the beginning of Blockchain technology. Although a great number of improvements were made, the first real-world application of Blockchain technology did not take place until 2008, when bitcoin was first introduced.

Blockchain can be used to transform a variety of fields, from healthcare and e-commerce to supply chain and polling or e-voting systems, by increasing transparency, reducing costs, and improving efficiency. This technology is able to revolutionize how we work and think in various sectors.

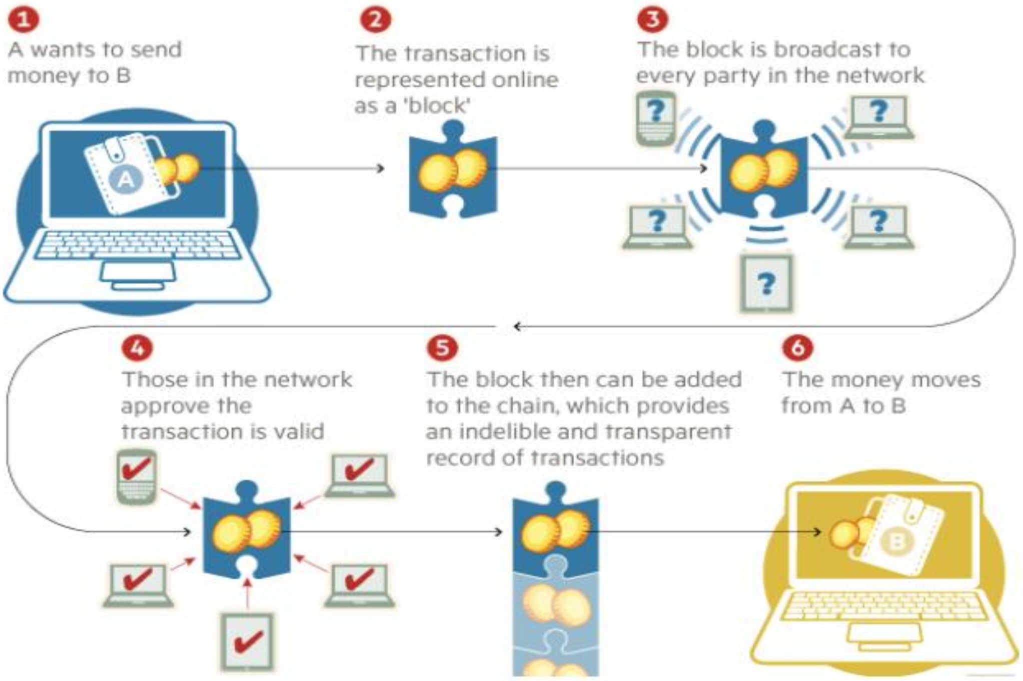

1
A wants to send money to B
A
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
?
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
B

Figure 1. How a Blockchain Works

Source: (Jane, 2015)

1.2 Non-Fungible Tokens (NFTs) and Fungible Tokens

NFTs erupted early 2021, which caught and attracted academics and business experts (Wired, 2021). Non-fungible tokens (NFTs) are digitized certificates of possession relying on "Blockchain technology". Having an NFT proves that you own a virtual asset you bought (Wang et al., 2021). Applications which relay on Blockchain, such as NFTs and fungible digital currencies (eg., bitcoin) that aren't NFTs, brought in about $2.5 billion in the first half of 2021. (Forbes, 2021).

An NFT, or non-fungible token, is a digital asset or token that is unique and cannot be exchanged or replaced with any other digital asset or token. It is distinguishable from other digital assets or tokens that are interchangeable (fungible). This is why the term "non-fungible token" is used. Typically, the record of the NFT's uniqueness is stored cryptographically on a Blockchain, and are of ease access to anyone. Though it's not always the case, NFTs are not just a virtualized data of an asset; NFTs are considered independent digital assets. To better understand the concept of NFTs, it may be helpful to compare them to fungible tokens or assets. Fungible tokens, which are common in the Blockchain world, are interchangeable and can be easily replaced by another identical token. A good example of a fungible asset is cash, as any ten-euro note can be exchanged for any other ten-euro note. Unique objects that can’t be replaced or can’t identical to others such as event tickets, art, collectibles, and ownership documentation (eg., land ownership) are examples of non-fungible tokens.

In order to make the benefits of NFTs more clear, let us first define a "token" as an object that possesses a specific and symbolic meaning (Oliveira et al., 2018). In the world of information technology, a collection of digital data that is used to identify a specific movable good is known as a "token." To be more specific, a token is a collection of digital data that is housed within a Blockchain and confers particular rights upon an object. The token in a non-fungible token transaction stands in for a certificate that verifies the originality, one-of-a-kindness, and ownership of a digital item. This item could be anything from a picture to an audio track, a movie clips to an online video game, or a tweet on one of the most popular social networking sites. In this way, the NFT makes it clear what a digital object's property is (Singh and Singh, 2021).

In a manner analogous to that of the products market, the products could either be fungible or non-fungible. Fungible tokens (FTs), much like fungible products, can be replaced but also quantifiable due to the very nature of the tokens themselves (e.g., a dozen eggs, an ounce of silver, a bag of potatoes) (Durham, 1965). The best-known examples of FTs are tradable cryptocurrencies like bitcoin and other tradable cryptocurrencies. The value of one dollar is always the same as the value of another dollar, and the value of one bitcoin is always the same as the value of another bitcoin. Due to the fact that they are fungible, they are a reliable method for carrying out transactions that make use of the same Blockchain technology as NFTs. In contrast to cryptocurrencies, non-fungible tokens cannot be traded in for other tokens of the same kind because the characteristics that distinguish them from one another are either coincidental or different (e.g., a ticket to a sold-out event or concert, rare collectible item, custom-made clothing, artwork, rare book or manuscript). Therefore, each asset has its own value due to the unique qualities it possesses. This is true whether the economic function of the asset is similar to other units (such as houses or buildings) or completely dissimilar (such as artwork or music tracks). The value of each asset is determined by its unique characteristics, regardless of its economic function relative to other assets.

When considered in this light, the potential of NFTs can be understood and appreciated. Ad hoc free online platforms (such as Google Images and YouTube) have been providing and selling digital items for decades, both illegally (such as on the black market) and legally (such as on Google Images and YouTube) (Wilson et al., 2021). In both scenarios, the material is simple to duplicate, and it can be difficult to determine whether or not it is authentic (Chohan & Paschen, 2021). Original owners of digital content, such as musicians, artists, and those who hold trademarks, have had a difficult time verifying their content and making a profit from it (e.g., digital movie or audio recordings and podcasts). clients have also had a hard time acquiring genuine digital content; up until recently, they were only able to have physical items like as labeled attire (Wilson et al., 2021). NFTs, on the other hand, allow businesses and companies for a new way to earn money their content while simultaneously assuring customers of their ownership of that content. In an effort to instill a sense of ownership in its customers, Taco Bell has sold non-food toys (NFTs) of individual taco pieces, and Pizza Hut has sold exclusive and rare NFT collections of pizza slices (Chohan & Paschen, 2021).

In light of the examples mentioned above, there is increasing interest in the use of NFTs to bring a shift regarding values and ideas behind a company's products or services. The majority of the momentum can be attributed to three distinct factors: the ability of creators to utilize and transfer the rights related to unique objects, the ability of users to show off their ownership of such objects, and the potential for marketing and advertising strategies to capitalize on the distinctiveness of such objects.

The Non-Fungible Token, also known as NFT, is a form of cryptocurrency that was derived from Ethereum's smart contracts (Fairfield, 2021: Wood, 2014). NFT was first introduced in Ethereum I'm Provident Proposals (EIP)-721 (William et al., 2018), and it was further developed in Ethereum I'm Provident Proposals (EIP)-1155 (William et al., 2018). Some examples of cryptocurrencies that use NFT include Bitcoin and Ethereum (Nakamoto, 2019). Bitcoin is a decentralized standard coin, which means that every coin is the same as every other coin and can be exchanged for another. In contrast, non-fungible tags (NFT) are one-of-a-kind and cannot be exchanged for items that are functionally equivalent; because of this, they are an excellent choice for unambiguously identifying anything or anyone. To be more specific, a creator can easily establish the existence and ownership of digital assets such as movies, photographs, art (Colavizza et al., 2020), and event tickets (Regner et al., 2019), amongst other things, by utilizing NFTs in conjunction with smart contracts in Ethereum. To elaborate, this allows the creator to create digital assets such as movies, photographs, and art. In addition, the inventor is eligible to receive royalties for each successful transaction that takes place on any peer-to-peer exchange or NFT market. The ability to trade full histories, the availability of extensive liquidity, and the simplicity of interoperability all position NFT as a potentially useful alternative for the protection of intellectual property (IP). NFTs are essentially composed of nothing more than codes, but due to the relative scarcity of NFT codes as digital assets, purchasers assign a monetary value to the codes themselves. It makes it possible for non-fungible virtual assets to trade at prices that were previously unattainable for certain intellectual property-related products, thereby effectively securing those prices (Witek, 2018; Shirole, 2020).

There has been expressed enthusiasm for a wide variety of non-traditional financial products (NFTs). They take part in activities related to NFT games or trades with a great deal of enthusiasm. One of the earliest Ethereum-based non-fungible tokens (NFTs), CryptoPunks is responsible for the creation of more than 1,000 collectible punks (6,039 males and 3,840 females) and contributed to the growth of the ERC-721 token card. Crypto Kitties (Wang et al., 2021) was a major reason for NFTs gaining popularity and headlines in 2017. The fierce competition among the participants for the rare cats resulted in a winning bid of more than 999 ETH (equivalent to $3 million USD).

The technologies are still in their infancy, despite the enormous potential impact that NFTs could have on existing decentralized markets and future economic prospects. Certain potential obstacles must be addressed, while positive prospects must be emphasized. In addition, despite the fact that a substantial amount of information on NFTs is accessible via blogs, forum posts, codes, and other sources, there is a lack of exhaustive research.

1.2.1 NFTs Vs. Fungible Tokens

There are several significant differences between non-fungible and fungible tokens. Similar to Bitcoin and fiat currencies, fungible tokens can be freely exchanged with other tokens of the same type.

Non-fungible tokens and fungible tokens differ in two significant ways. Non-financial transactions are distinct and cannot be divided or merged. In a Blockchain network, An NFT represents ownership of a virtual asset, for example, a virtual collectible, art, or any other digital certificate of ownership. It allows for the verification of ownership of digital items (Mahdad, 2021). In 2017, the first NFT was issued on the Ethereum ERC 721 platform. NFTs have various novel use cases compared to fungible tokens, such as showing game valuables, tokens related to fans in which they can boast about, and art (Parham & Breitinger, 2022).

Understanding the economic concept of fungibility can be helpful in comprehending NFTs and non-NFTs (FT). The main comparison goes with crypto tokens; in which they demonstrate their fungibility by a script of code. Non-NFTs (FT)s such as a euro note is interchangeable and not unique. For example, a one euro note either in France or Germany are the same and can be exchanged and still have the same value.

A non-NFT (FT) can be crypto coin (eg., Bitcoin). No matter where it is issued, one bitcoin is worth one bitcoin. On the contrary, non-fungible, they can be thought of as a type of title ownership for a one-of-a-kind, an asset that can’t be replicated or to have two and more of. A ticket of a football match is an example of non-fungible since its unique data means it cannot be duplicated. Houses, boats, and cars are non-fungible physical assets because they are unique. The same is true for non-fungible tokens (NFTs), which could be thought of a single, unique item.

Blockchain technology can be used to verify ownership of virtual assets. The biggest distinction of fungible and non-fungible tokens is the information they contain. Bitcoin, a fungible token stores value, and non-fungible tokens stores data such as artwork or a school certificate.

In 2012, the notion of “colored coins” was introduced to the Blockchain of Bitcoin, non-fungible tokens have been around. It would make the attachment of metadata that provides additional data used for Bitcoin exchanges possible, rather than building additional Blockchains as sidechains.

While colored coins can be used to portray real-world objects that are exchanged on the Blockchain of Bitcoin, they are bonded with an external contract and require a foundation of trust to be valid. There must be a consensus among the group that a specific quantity of colored coins represents a different value. As a result, it is possible to use these "labeled" coins to conduct transactions in the value in question.

The digital tokens being used are called Satoshis, which are very small fractions of a bitcoin. These Satoshis have been "colored in" with data that links the coins to physical assets in the real world. The colored coins utilization is confined in the cryptocurrency field. They were mainly used on a P2P (Peer-2-Peer) trading platform built on the Bitcoin Blockchain, to create and exchange art like digital cards called "Rare Pepe."

On the Ethereum Blockchain, the first non-fungible tokens were generated, which can be used to generate a one-of-a-kind identifier for a good, a service, or an individual. Voting tokens are stored on the Tron and EOS Blockchains, which are used to construct some NFTs. There are practically infinite applications for this type of token, from lottery tickets to concert and sporting event seats to collectable items like artwork and musical compositions.

On the Blockchain, non-fungible tokens (NFTs) can also operate as marketplaces for the storage of academic titles and digital identities due to the fact that they are simple to verify and track. Following the phenomenal market growth that NFTs experienced in 2020 and 2021, there is a misconception regarding NFTs, specifically the perception that they are only artworks. NFTs, on the other hand, were extensively used in the gaming sector long before art had started getting involved.

1.2.2 The Origin of NFTs and Their Characteristics

The proliferation of NFTs started in 2017 and can be traced to the "CryptoKitties" craze. The Canadian company Dapper Labs created CryptoKitties using non-fungible tokens (NFTs) as part of a game (Serada et al., 2021). These figurines were all distinct and tradeable, similar to collectibles. Numerous digital creators have begun submitting their content within the NFT format in an effort to produce irreplaceable, unique content by leveraging CryptoKitties experiences. Such efforts have gained great interest by users and the media and have had an impact on a variety of creative markets, including the visual arts, clothing and apparel, and music industries (Wang et al., 2021).

Mike Winkelmann, also renowned as Beeple, a digital artist sold a non-fungible token (NFT) made up of a collection of 5,000 special digital creations in the shape of pictures, that are created in a period of thirteen years, for nearly $70 million (Forbes, 2021). Banksy, a new rising artist, destroyed one of his digital works in a live stream to ensure the uniqueness of the tokenized digital copy. The item was then sold for four times its original price on a digital marketplace. OpenSea, Rarible, and SuperRare are among the most popular marketplaces for these NFTs. By mid-2021, each will have recorded transaction values by dozens of millions. (Focus, 2021).

On online platforms, FTs and NFTs operate quite differently from one another in significant ways. NFTs cannot be traded for one another, and as a result, they are not divisible at all. This is in contrast to fractional FTs, which can be traded (Wang et al., 2021). A non-fungible token can be considered and understood as a proof of ownership which is unambiguously, specifically, and unquestionably establishes who the owner of an item is (Ante, 2021). NFTs, are also utilized to build and perform "scarcity", to prove the ownership of a virtualized token across multiple platforms (Chohan and Paschen, 2021).

NFTs is developed and implemented on-chain in compliance with specific frameworks or standards. At the moment, Ethereum’s Blockchain is the most used Blockchain for NFTs, and Ethereum's most popular protocol, ERC-721, it gives certain characteristics to NFTs. Thus, NFTs can be managed, exchanged, and held in accordance with the framework or protocol's established attributes.

The concept that evolved into today's NFTs dates back to 2012, when the bitcoin community debated "colored coins." Because bitcoins are fungible, meaning they cannot be distinguished from one another, the concept of colored coins was simple yet novel. By methodically tracing a bitcoin's origins, it was discovered that it was possible to differentiate the coin from others by labeling it with "color." This innovative idea was applied to virtualized collectibles, currencies, and the issuance of firm stock. Despite numerous research studies, including one by Ethereum's founder, Vitalik Buterin, the concept of colored coins never materialized due to opposition from the bitcoin community. It did, however, lay the foundation for NFTs.

Cryptographic tokens with a single, immutable value are known as non-fungible tokens (NFTs). This item is rare because it is unique and cannot be exchanged for anything else. Also, NFTs can be digitally made or adapted of physical content (Evans, 2019; Wang et al., 2021). NFTs in a simple manner are virtual tokens which can be bought, exchanged, and traded thanks to their special properties (See Table 1).

Table 1. Properties of NFT

Properties of NFT	**Meaning**
Unicity	Meaning that NFTs can't be identical, since NFTs have unique identifiers. This ensures that each NFT is one of a kind.
Indivisibility	The NFTs may be subdivided, but the exchange must be conducted with the full amount. Consequently, it is impossible to possess a part or a portion of an NFT.
Scarcity	NFTs are uncommon since a single NFT of its kind ever exists.

Sources: (Sestino et al., 2022)

NFTs could be considered as one of the most valuable components of Blockchain, both of which are gaining traction in a variety of fields across the world. NFTs are also becoming increasingly popular. First proposed on the Ethereum Blockchain (EIP-721), NFT is an offshoot of Ethereum's smart contract functionality. NFTs are their own unique thing, standing in contrast to cryptocurrencies like Bitcoin. Non-fungible tokens, also known as NFTs, are distinct from one another and cannot be duplicated in the same way that digital coins can. The ownership and existence of virtualized (eg., clips, photos, artwork, and a flight ticket) amongst other things, are represented by NFTs (Wang, 2021).

As of now Ethereum is the most popular Blockchain which supports NFT. Ethereum supports the necessary smart-contracts to mint and create NFTs. However, Ethereum is not the best in every way, as it has several significant flaws. We investigate the Ethereum Blockchain's most significant challenges and issues, such as high transaction fees and slow transaction times. This necessitates the use of alternative Blockchain networks or the upgrading of their protocols. However, there are other Blockchains such as Cardano, Polkadot, and Ethereum 2.0, support the architecture of NFTs. These Blockchains could help resolve the issues with the Ethereum Blockchain, and in the future, they could serve as alternatives or competitors to Ethereum.

1.2.3 Technical Components of NFTs

NFT depends on three major technologies, we will briefly explain each.

1.2.3.1 Blockchain

A Blockchain is a distributed ledger that keeps track of transactions (called blocks) through an anonymous p2p network (Huaimin et al., 2018). Since adding new information to the end is the only way to make changes, the size of the database grows with each transaction. Ethereum is the most popular Blockchain used for NFT because it makes it safe for smart contracts to be carried out.

1.2.3.2 Smart Contract

Smart-contracts are similar to real-world contracts, but instead a digital-world. Smart-contracts are applications that are stored in a Blockchain (eg., Etheruem's Blockchain) (Zheng et al., 2020). If a specified requirements and terms are fulfilled, the contract is immediately enforced. It uses scripting languages that are Turing-complete to implement complex functionality and carry out exhaustive state transition replication using consensus algorithms to make sure that the final state is always the same.

NFTs depend on the Blockchain that use smart contracts to ensure the orderly execution of transactions. To hasten, verify, or carry out digital negotiations, "smart contracts" were first proposed in 1996 (Szabo, 1996). The smart contract features of the Blockchain were improved by Ethereum.

Smart contracts make it possible for parties who can't be trusted or who are spread out across a network to trade fairly without a central authority.

1.2.3.3 Addresses

Blockchain addresses are fundamental topic. An address is used to receive or send assets whether they are crypto coins or NFTs, think of it as an email address but for digital assets. An address is usually a string of letters and numbers, and it is generated by a cryptographic function that ensures that it is unique.

An address is used to identify the owner of a particular NFT and to track the movement of the NFT from one owner to another. When an NFT is minted, it is assigned a unique address that is stored on the Blockchain. This address is then used to track the movement of the NFT as it is bought and sold on the open market.

The task of transferring ownership is usually done with the help of a cryptocurrency wallet. It typically includes a public address and a private key, which are used to sign and verify transactions. The transmission of a transaction involving smart contracts follows the ERC-777 token standard (Jacques et al., 2017).

ERC-777 token standard is a specification for the making of smart-contracts that define the functionality of a token on the Ethereum Blockchain.

1.2.4 Technicalities of NFTs

The fundamental pillars of the underlying technology, in this case known as "Blockchain," are responsible for determining the distinguishing attributes of NFTs (Wang et al., 2021). The Blockchain is a decentralized system for recording and verifying transactions that can be used for many different purposes, such as the registration of authenticity, history and origin, and property (Whitaker et al., 2021). It refers to a collection of software programs that save information in records that are laid out in the form of blocks (hence the name). Every single transaction block that has been finished and validated is connected to the one that came before it in the chain all the way up to the most recent block. Data can be stored in a way that is immutable, transparent, and decentralized using Blockchain (O'Dwyer, 2020). (Because the Blockchain is supported by cryptographic protocols, committing double spending or deleting newly recorded transactions from the ledger is extremely difficult, if not impossible.) Transaction information is dispersed across a large number of network nodes or copies of the Blockchain in identical form (Gorkhali et al., 2020; Pilkington, 2016).

To make things easier to understand, the data handling process in a Blockchain can be divided into seven steps:

1. Create a data entry in which data is requested and authenticated (in the form of a transaction).
2. Creation of a block that represents the transfer.
3. Transmission of a block to all nodes (all network participants).
4. Transaction verification through nodes of the networks.
5. Reward distribution and payments to nodes for chain verification.
6. A new block is added to the Blockchain using a set of procedures.
7. Update is distributed to the entire network.

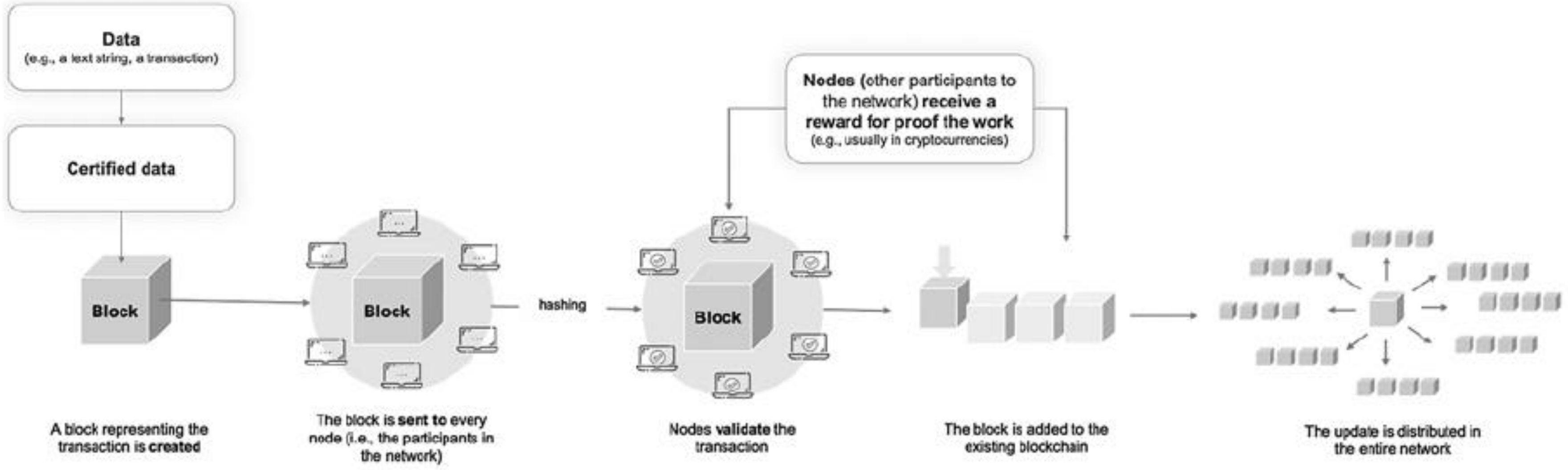

Data
(e.g., a text string, a transaction)
Certified data
Block
A block representing the transaction is created
Block
The block is sent to every node (i.e., the participants in the network)
hashing
Block
Nodes validate the transaction
Nodes (other participants to the network) receive a reward for proof the work
(e.g., usually in cryptocurrencies)
The block is added to the existing blockchain
The update is distributed in the entire network

Figure 1. The Data Management Process in The Blockchain

Sources: (Sestino et al., 2022)

A "hash" is a unique number used to track and validate the creation of blocks. This is accomplished with the assistance of algorithms that ensure the information being tracked is unique (Gupta, 2017; Seok et al., 2019). A "hash" is a type of cryptographic technique that uses a mathematical formula to transform a particular type of data (such as a message) into a "hash value" a binary string of specific length (also named a "digest"). Because this string is unique, it protects individuals' private information (Singhal et al., 2018). Hash function has the ability to convert any string of characters into a one-of-a-kind combination of letters and numbers.

For example, the word "Jordan" could create a code such as "ABC123AB." The data can be verified with these hashes, and a Blockchain block can be generated. After the data is verified, all nodes in the network receive the block. The nodes network contains all the machines (additionally, by extension, people) linked together (Nofer et al., 2017). All connected nodes can verify transactions before adding to the distributed ledger (Maxmudjanovna et al., 2020). Technically, all members have access to the register's information, which is accessible, transparent, and simple to locate. Furthermore, once data is registered in the Blockchain, it is unable to be changed without all network’s consent (Pilkington, 2016).

This technique could help authenticate and confirm various business applications because of the secure nature of its transactions. Consider how the Blockchain creates a link of blocks connected by a unique hash and then replicates it n times across the network. Therefore, the network's certification hash must also be modified if a single data block is modified. The blocks in the chain are connected by inserting the previous hash into the n-1 position of the block. If any change is made, it is instantly reflected in all subsequent blocks on the network. Changing the chain fraudulently is nearly impossible because it is difficult and must occur simultaneously across the entire chain.

This procedure makes sure that networked data can't be changed and enables the possibility of having different variety of programs (Saberi et al., 2019; Zhai et al., 2019). So far, management of supply-chain is a very popular business that uses of Blockchain. This includes figuring out where items are in the supply chain, keeping an eye on product quality, and preventing losses.

In the field of FTs, the primary purpose of FTs is to promote and manage cryptocurrencies such as Bitcoin. The first "digital" coins that rely on Blockchain were Bitcoin and Ether (the digital currency of the Ethereum). Despite Bitcoin and Ether using Blockchain technology, they are distinct and serve different purposes (Song et al., 2019). The first decentralized cryptocurrency was bitcoin, unaffiliated with a government-controlled financial institution or a country (Ciaran et al., 2016; Dwyer, 2015). Ethereum is a distributed Blockchain platform that can be used to develop applications. Ethereum is significantly more robust and can be viewed as Bitcoin 2.0, allowing dApps (decentralized Applications) to be constructed on its foundation.

Additionally, there is a great deal of opportunity for both private and public organizations to use applications based on the Blockchain. During a referendum, for example, states and countries can convert online voting into a Blockchain-powered transaction that verifies the legitimacy of a voter's vote (Park et al., 2021). In a situation like this, Blockchain has the ability to make polling more transparent by enabling regulators to observe network changes immediately. Documentary certification is an additional alternative. Educational programs and written materials, for example, can be accredited. This could be utilized in data analysis and study (Shah et al., 2021), titles of ownership (Themistocleous, 2018), the ability to track medicines (Sylim et al., 2018), and the creation of mobile software that make customers and users feel more secure regarding information security (Sestino et al., 2022). The Blockchain is considered a very trustworthy technology and method for securing information in the absence of a governing authority due to its reliance on the immutability of information.

1.2.5 The NFTs' Creation Process

Numerous Blockchain marketplace platforms, such as Meta Mask, Bit ski, and OpenSea, enable the creation of NFTs (Forbes, 2021). When a user uploads a file, these platforms ensure the file is transformed to a Blockchain-powered asset and vouch for its distinctiveness. For clients, generating an NFT through these platforms usually requires a set of steps.

Accessing the chosen platform and creating a user account, profile, and "virtual wallet" are typically the tasks involved in the first step of the process. To get started, an email address is typically all that is needed of a user in the vast majority of instances. In the second step, user selects an NFT along with the target file format (for example, an image, video, audio, or document. The last step in the process requires users to give the digital item a name, supply a succinct description, and supply a URL to a personal website (such as social media profile). Users will then transfer the file which then will be modified using Blockchain technology during the fourth phase (as described below). The user has the option of including a payment reward or transaction fee once the NFT has been created (in the Ether currency). Once that is done, the NFT can be purchased, exchanged, or given as a gift through the platform's market. or through an automated link that can be distributed across the most popular social media sites. As soon as the transaction for the sale of the virtual good has been completed, for instance, the user will hand over both the non-fungible token (NFT) and the verified deed to the purchaser of the virtual good. Figure 3 provides both step-by-step instructions as well as a visual representation of the process.

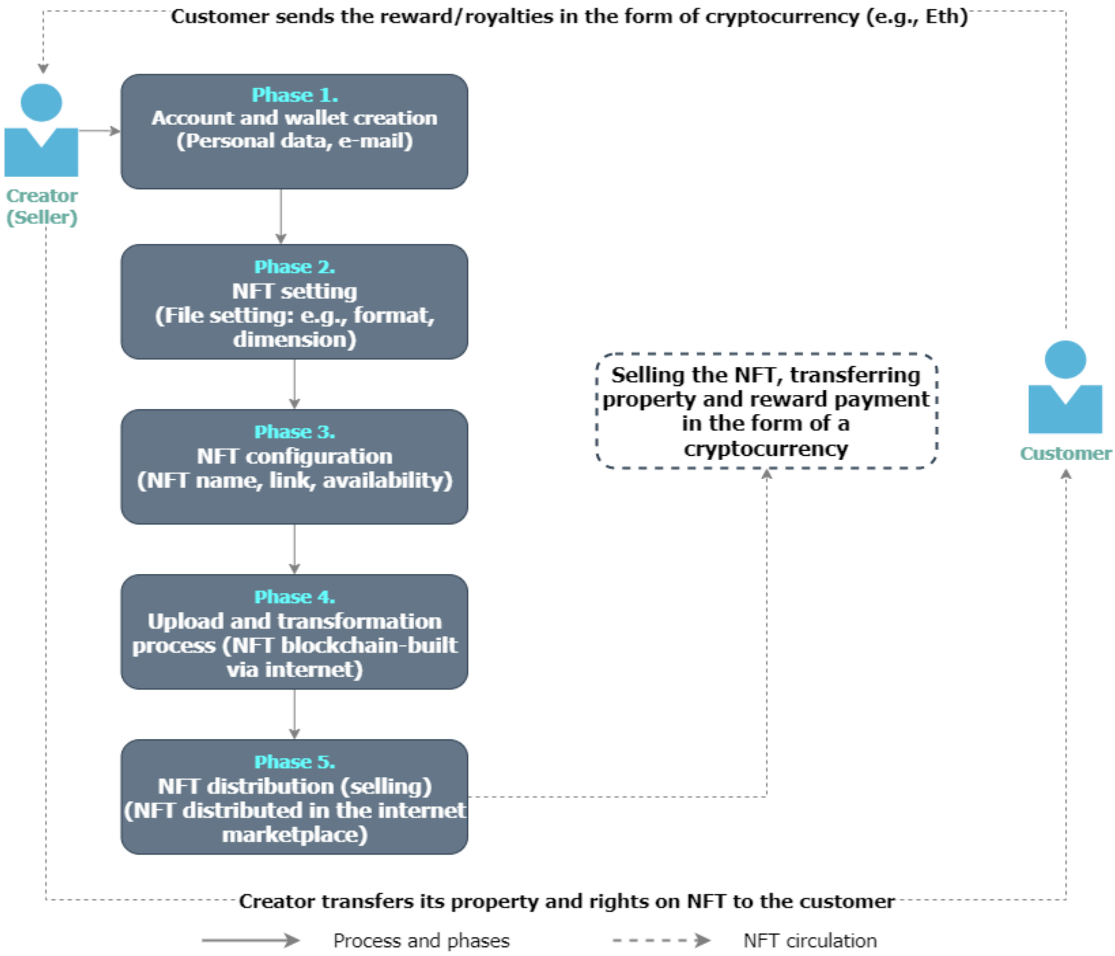

Customer sends the reward/royalties in the form of cryptocurrency (e.g., Eth)
Creator (Seller)
Phase 1.
Account and wallet creation (Personal data, e-mail)
Phase 2.
NFT setting (File setting: e.g., format, dimension)
Phase 3.
NFT configuration (NFT name, link, availability)
Phase 4.
Upload and transformation process (NFT blockchain-built via internet)
Phase 5.
NFT distribution (selling) (NFT distributed in the internet marketplace)
Selling the NFT, transferring property and reward payment in the form of a cryptocurrency
Customer
Creator transfers its property and rights on NFT to the customer
Process and phases
NFT circulation

Figure 3. Five Phases in The NFT Creation Process

Sources: (Sestino et al., 2022)

1.3 Marketplaces

Marketplaces are platforms that enable users to buy, sell, make, and trade non-fungible tokens (NFTs), example of non-fungible tokens marketplaces (NFTMs) include; Rarible, SuperRare, and OpenSea (Bhujel & Rahulamathavan, 2022). We will focus on OpenSea since it is the most popular marketplace.

1.3.1 Understanding OpenSea

OpenSea is extremely proud of the fact that it was the first and is the biggest NFTM that offers necessary NFT solutions. OpenSea was created in 2017, no place before it people could easily trade different non-fiat currencies. OpenSea was created as a way for users to trade crypto collectibles and other non-fungible tokens (NFTs) with each other (Das et al., 2022).

Both computer and smartphone graphical user interfaces begin with different windows that allow users to either investigate NFTs or generate a cryptocurrency wallet. User also has the option of connecting his existing cryptocurrency wallet to the platform if you have one already. User can either look through the more than 2 million NFT collections already available or make your own (Das et al., 2022).

OpenSea works with many different kinds of non-fungible tokens (NFTs), such as assets that represent different works (eg., artworks, collectibles, virtual lands) and more.

Users are able to quickly recognize the best and most fashionable collections in each category. Search results can be adjusted and decresed by selecting different range of times. There is also the possibility for users to choose a specific Blockchain that users would like to investigate (Yoder, 2022).

1.3.2 How to Use OpenSea

OpenSea features a user interface that is both easy to use and approachable for newcomers, making it a breeze to operate and navigate. To begin using OpenSea for transactions, you must first link a cryptocurrency wallet to the platform. Your wallet is the interface through which you interact with the Blockchain in order to send and receive deposits and payments. Whenever a user connects his wallet with OpenSea, non-fungible tokens (NFTs) are not kept on OpenSea, as OpenSea is a non-custodial platform; rather, they are sent to the address you provided for your wallet.

1.3.3 Connecting to OpenSea

The procedure for connecting to OpenSea is the same regardless of which cryptocurrency wallet you use, be it MetaMask, Coinbase Wallet, or any of the other wallets.

Go to OpenSea.io, find the section labeled "My Wallet" at the window bar, and then press the kind of wallet that you want to use. When you are ready to connect to the platform, the prompt for entering your private keys will appear on the screen of your device. In order for your wallet to successfully connect, you are going to need some Ethereum (ETH) (White & Passi, 2022).

After successfully connecting to the platform, you will be able to access the page of your account where you can view all of the NFTs that you currently possess. You have complete freedom in the manner in which you trade or sell your NFTs within the marketplace. Information such as account name, email, URLs to your social media accounts can all be entered into the profile section.

1.3.4 Searching for NFTs on OpenSea

If you want to look through all of OpenSea's NFTs, the "Explore" tab is the place to go. Collections can be viewed by either selecting a specific category or by searching for a specific NFT.

Popular NFT groups, some with moving and moving ones, light up the page. The "Trending" category includes well-known libraries such as "Decentraland" and "Bored Ape Yacht Club" (White & Passi, 2022).

The “Stats” page also allowed you to look for NFTs. The top NFTs from the past day are displayed by default, and it has more analytics features. Use the volume, time, category, and Blockchain tabs to refine your search.

2. SECURITY AND PRIVACY CHALLENGES OF NFTS

The Blockchain is still considered a recent innovation which first gained popularity as the foundation that underpins the digital currency Bitcoin, which was introduced in 2009 amid the economic crash. Blockchains are public ledgers that contain all of the transactions that have ever been made using Bitcoin (Nakamoto, 2008; Zohar, 2015). With the initial integration and the introduction of crypto coins, a broader range of software applications have emerged that are able to run certain sections of code on a Blockchain. This ability has allowed for the development of a number of different types of applications (Beck, 2016). In the year 1994, Nick Szabo was the one who first used the term "smart contracts." They make it possible for parties that are unfamiliar with one another and do not trust one another to engage in secure transactions together. Consistency is achieved through the use of a consensus protocol that is distributed among all of the nodes participating in the underlying Blockchain (Glaser, 2017; Sillaber & Waltl, 2017).

Established business models that rely on third parties for trust may be susceptible to disruption or even complete replacement as a result of the technology known as Blockchain. When the whitepaper for Bitcoin was published in 2008 (Nakamoto, 2008), it established the concept of Blockchain. For the first few years after its inception, Blockchain was primarily utilized to support cryptocurrencies. Few years later, a new generation of Blockchains was released (eg. Ethereum 2014), It enabled the programming and execution of applications known as smart contracts across all nodes involved in Blockchain. This was made possible by the introduction of Blockchains, which allowed for the execution of smart contracts. Therefore, anyone could design and implement programs on a worldwide network that is obtainable with users (Buterin, 2014; Wood, 2014). Logistics, cross-border payments, international trade financing, and energy markets are just some of the industries that have seen the development of novel concepts aimed at simplifying human interaction and collaboration on a large scale (Schweizer et al., 2017).

A better understanding of NFTs will help us research in three ways, except for the fact that the first experimental use cases are already available. To start with, having a good understanding of the common characteristics of NFTs and the differences to fungible and non-fungible tokens helps you understand the rewards and possibilities that come with them. Second, both researchers and people who work with NFTs benefit from having more detailed information about how to make and evaluate applications based on NFTs. Third, knowing more about practical problems helps future researchers focus more on solving the rest of the problems. It's a shame that academic researchers aren't studying NFTs in more depth to look at these issues. Furthermore, there isn't enough information about recommended strategies, projects, and how to build applications on the Blockchain in the world right now (Delmolino et al., 2016). As a result, we find that there is a big gap in research.

There needs to be more empirical research on the benefits and drawbacks of NFT use to date. NFTs may enable previously unimaginable use cases and provide value to users, even though they are not valuable in and of themselves (Sparango, 2018).

Even though NFTs have garnered considerable attention in a short period, they are still in their infancy and should not be taken for granted. There are still numerous obstacles to overcome and opportunities to investigate. We intend to highlight the challenges of NFT, and discuss how to mitigate and thwart them if applicable.

2.1 Security Challenges

The NFT technology hasn't grown yet, and has a long road to go before reaching maturity. As such, we will discuss the security challenges inherent in NFT and show the defense measures available to address them.

There are many factors to consider when dealing with non-fungible tokens. It is essential to conduct extensive research on tokens, creators, artists, use cases, and marketplaces. There is never a guarantee of success in this industry, but all of these factors will determine whether the asset you wish to acquire is worthwhile.

The price potential of NFTs attracts many individuals. Early investors have reaped profits from popular and notable groups of NFT such as Bored Ape. Nonetheless, there are dozens of failed projects for each successful collection, at least in the short term.

Sadly, there are a multitude of additional potential issues to consider. NFT spoofing is one such concern. It is a common practice for marketplaces to host fake NFT stores that replicate existing projects. It is similar to phishing websites, although criminals are not interested in login credentials. Instead, they will deceive unsuspecting users into buying worthless artwork.

We are going to divide the security challenges into three segments:

- Blockchain and smart-contracts related challenges
- Platform related challenges
- Users and user's wallets related challenges

In each segment we will talk about different challenges and mitigations or solutions if possible

2.1.1 Blockchain and Smart-contracts Related Challenges

Denial of Service Attack: A denial-of-service (DoS) attack is a type of network attack in which an attacker attempts to interrupt the on-going operations of a server to make it unavailable to the genuine audience (Horizen, 2022). DoS attacks impede access and disrupt the NFT service, which unauthorized users could exploit. Thankfully, the Blockchain makes user actions readily accessible. Users with proper authorization can access the data as needed, and data loss is not caused by human error. DoS attacks on websites or data laying outside of the Blockchain could render the NFT system inoperable.

Blockchain networks can be protected from DDoS attacks in multiple ways. A decentralized network architecture, in which the network is randomly distributed across multiple devices and locations, is one approach (Rodrigues et al., 2017). This makes it harder for attackers to target a single failure point. Implementing rate limiting and filtering measures can also help prevent DDOS attacks by limiting the volume of traffic.

A centralized network of nodes controlled and handled by a credible intermediary is an alternative method. This can prevent nodes from being compromised and reduce the likelihood of a DDOS attack (Swami et al., 2019).

Another approach is to use Blockchain-specific technologies, including consensus mechanisms such as proof-of-work or proof-of-stake, to secure the network. These algorithms require participating nodes to prove that they have performed a specific amount of computational work in order to contribute in the network. This can make it more difficult for attackers to gain control of a large number of nodes and launch a successful attack.

It's also important for organizations to implement strong security measures (eg., firewalls and IDS), to protect their own systems from being compromised and used in DDoS attacks.

%51 Attack: Blockchain networks are at risk of being attacked. A 51 percent attack occurs when malicious miners gain control of over half of the network's mining hash rate or computing power. This allows the attackers to block the confirmation of new transactions or even halt them completely. (Ye et al., 2018).

The Bitcoin Blockchain is unlikely to be the target of a 51% attack due to its widely decentralized nodes and high hash rate. For that it is nearly impossible to be attacked, as the malicious actor would need a substantial amount of computing power and resources.

The more decentralized a Blockchain network is, the less likely it will be attacked. In conclusion, it is highly unlikely that a Blockchain network like Ethereum will experience an attack (Lin & Liao, 2017).

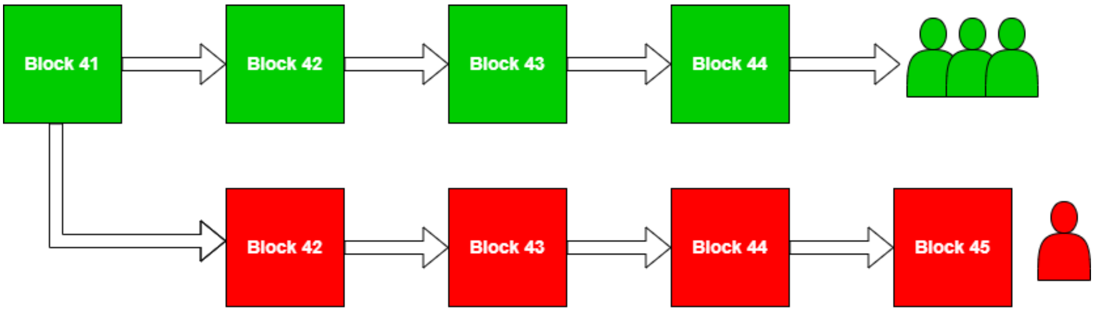


Figure 4. A 51% Attack Example

Source: (Horizon, 2021)

In Figure 4, the malicious (red) miner has more hashing power than the legitimate miner, they can add new blocks to their own private chain and broadcast it to the rest of the network once it becomes longer (heavier) than the original chain. In this way, they can potentially disrupt the integrity of the Blockchain. (Jimi, 2018).

Sybil Attack: A Sybil attack is a way to manipulate a peer-to-peer network by making many fake identities. These identities show as a regular client to the observer, but a single entity controls them all behind the scenes. One potential use for Sybil attacks is to censor certain participants on the network. A number of Sybil nodes can surround a target node and inhibit its ability to connect with other honest nodes, effectively blocking the target from sending or receiving information to interfere with the communication in the (P2P) network. This attack is also called an Eclipse Attack (Swathi et al., 2019).

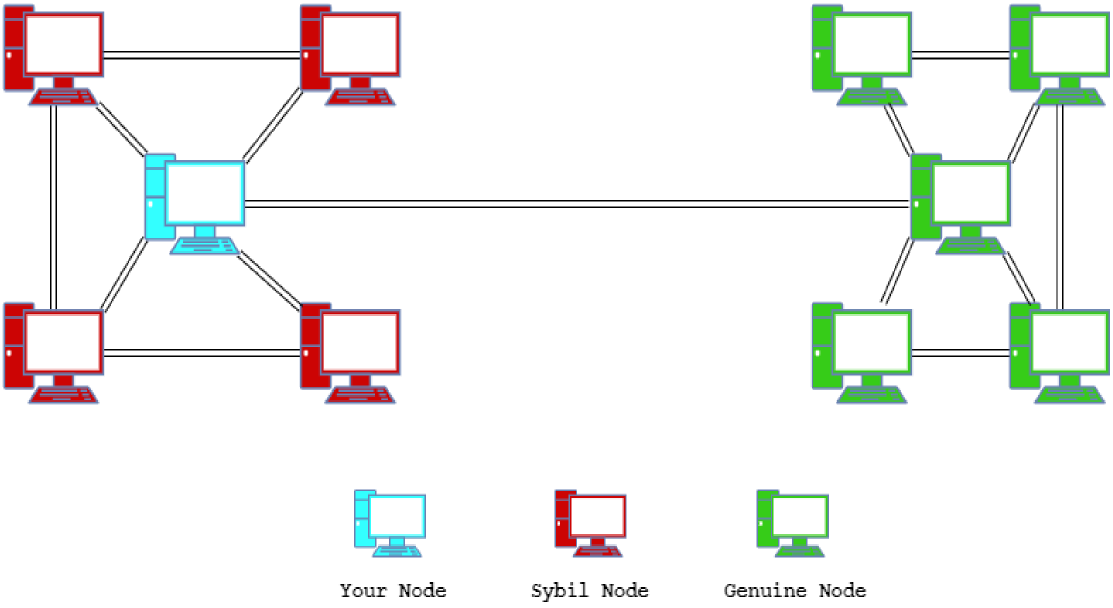


Figure 5. Sybil attack scenario on a Blockchain

To mitigate the risks of a Sybil attack, the cost of creating an identity on the network can be increased. This cost must be carefully balanced to ensure that new users can still join the network and create legitimate identities, while making it expensive for attackers to create a huge quantity of fake identities in a brief time frame.

In proof-of-work (PoW) Blockchains, the nodes that make decisions on transactions are the mining nodes. There is a real-world cost associated with creating a fake mining identity, such as buying mining hardware and consuming electricity. Additionally, having a large number of mining nodes does not necessarily give an attacker enough influence over the network. To do that, the attacker would also need a significant amount of computational power, which would be prohibitively expensive (Swathi et al., 2019). These costs make it difficult to Sybil attack PoW Blockchains.

Re-Entrancy attack: In computer science, a re-entrant process is one that can be interrupted during execution and then restarted without error. A hacker's attack of this nature can result in serious vulnerabilities. The most prominent example of this is the DAO hack, in which $70 million worth of ether was stolen. The Ethereum Constantinople hard fork was recently postponed following the discovery of a reentrancy issue during the launch's final stage (Moubarak et al., 2018).

A simplified example of how the malicious attacker can do a Reentrancy attack is as follows (Holds, 2019):

1. The attacker identifies a weakness in a smart-contract that leads them to repeatedly call a specific function in the contract.

2. The attacker creates a malicious contract that repeatedly calls the vulnerable function in the target contract.
3. The attacker uses the malicious contract to send multiple transactions to the target contract, triggering the vulnerable function each time.
4. The target contract processes the transactions but does not have any protections in place to prevent the same function from being called multiple times.
5. The attacker is able to repeatedly call the vulnerable function, allowing them to perform malicious actions, such as stealing funds or modifying data.

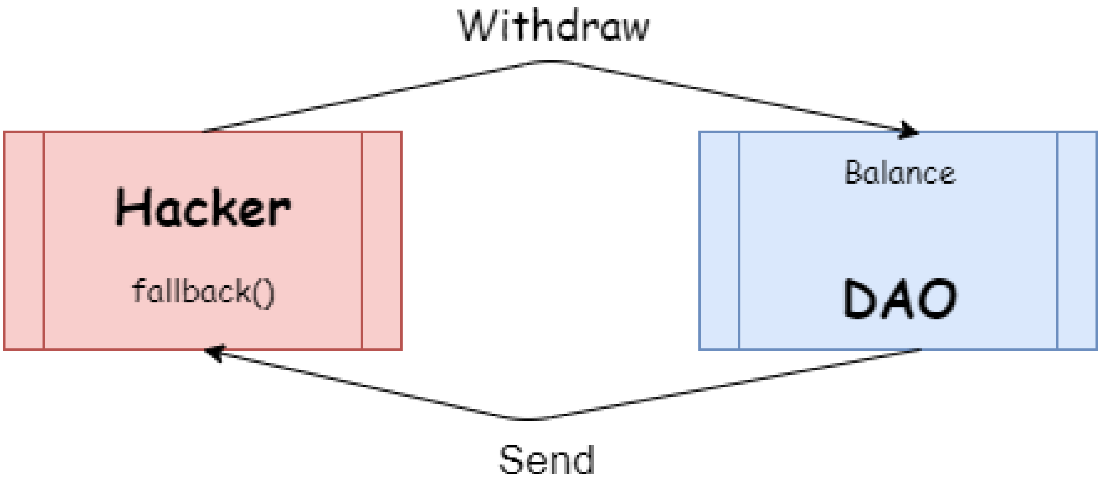


Figure 6. A Simple Illustration of Re-Entrancy Attack

Sources: (Pratap, 2022)

In figure (6), an attacker uses a flaw in the smart contract to drain the DAO's funds by repeatedly calling the withdraw() function. The main problem is that the contract does not update the hacker's account balance until the ETH-sending transaction completes. However, the transaction cannot complete until the hacker's fallback function completes execution. This creates a loop that allows the attacker to keep calling the withdraw() function and receiving ETH without decrementing their balance, thereby draining the DAO's funds.

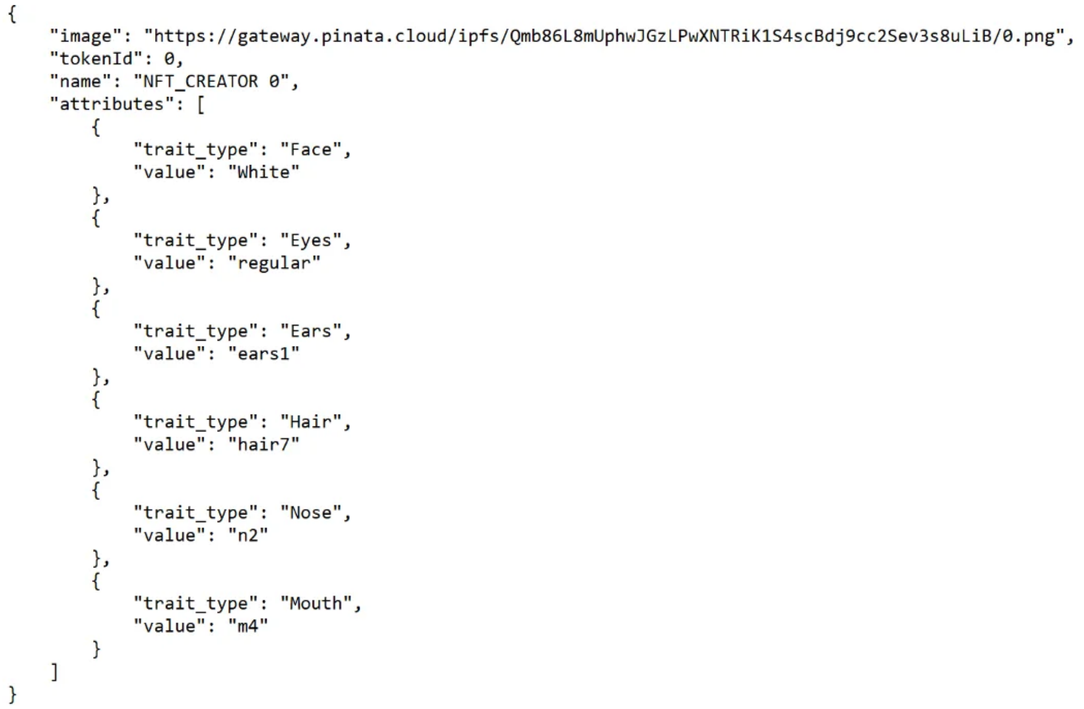
To prevent this type of attack, smart contract developers can implement safeguards to prevent functions from being called multiple times, or to limit the number of times a function can be called in a given time period (Krupa et al., 2021).

Tampering and Editable Meta-data: Damage to the integrity of NFT data can be caused by tampering (Ante, 2021). Assume that the hash algorithm used in the Blockchain is both preimage and second preimage resistant and that the Blockchain is a highly secure public ledger of transactions (Atzei et al., 2017). Once a transaction is confirmed, no unauthorized changes can be made to the NFT's metadata or ownership. Unfortunately, information not kept in a distributed ledger (Blockchain) and can be tampered with. However, there are places where NFTs' metadata can be modified (Das et al., 2021).

The specific steps of an NFT tamper attack will vary depending on the specific details of the attack, but here is an example of how such an attack might work:

1. The attacker identifies a vulnerability in the security measures that are in place to protect an NFT and its associated digital assets. This could include a vulnerability in the platform or infrastructure that is used to store and manage the NFT, or a weakness in the cryptographic techniques that are used to secure the NFT's digital assets.
2. The attacker uses this vulnerability to gain unauthorized access to the digital assets associated with the NFT. This could involve using a variety of techniques, such as exploiting software bugs, using social engineering tactics, or using advanced hacking tools and techniques.
3. After the attacker has gained privilege to the NFT's digital assets, they can begin to modify or alter them without the permission of the original creator or owner. This could involve changing the digital artwork or other content associated with the NFT. or altering the metadata or other information that is stored on the Blockchain.
4. The attacker may then attempt to sell or distribute the modified NFT to unsuspecting users or use it in other malicious ways. For example, the attacker could attempt to sell the modified NFT as the original, unaltered version, or use it to damage the reputation of the original creator or owner.

There are two ways to alter or tamper with the data. One is by changing the token's metadata through its corresponding URL. The other way is by altering the metadata issued on other domains, which can still be changed or deleted even if the smart-contract blocks the first method. All it takes to do this is to hack the domain.



```
{
    "image": "https://gateway.pinata.cloud/ipfs/Qmb86L8mUphwJGzLPwXNTRiK1S4scBdj9cc2Sev3s8uLiB/0.png",
    "tokenId": 0,
    "name": "NFT_CREATOR 0",
    "attributes": [
        {
            "trait_type": "Face",
            "value": "White"
        },
        {
            "trait_type": "Eyes",
            "value": "regular"
        },
        {
            "trait_type": "Ears",
            "value": "ears1"
        },
        {
            "trait_type": "Hair",
            "value": "hair7"
        },
        {
            "trait_type": "Nose",
            "value": "n2"
        },
        {
            "trait_type": "Mouth",
            "value": "m4"
        }
    ]
}
```

Figure 7. An example of the NFT metadata

Sources: (Patel, 2022)

The metadata URL must be protected within the smart contract to prevent the first hacking method. To reduce the risks of the second method, metadata should be uploaded to IPFS. This is beneficial because the cache of the content is included in the URL address of the file with metadata. Therefore, the metadata cannot be altered without changing the NFT's URL (Musienko, 2022).

In order to protect your NFTs from these dangers, you should use a platform such as CryptoPunks, Foundation, or Nifty Gateway. They forbid altering the metadata URL in their token contracts. Xie's platform is experiencing problems because its token agreements allow users to alter the URL address. Creators can update the metadata URL prior to the initial sale on OpenSea, SuperRare, and Sorare. However, only the platform Foundation demands the need of IPFS-based metadata storage.

Lost Control Over Execution: Smart-contracts can sometimes be altered or manipulated in a way that causes them to stop functioning as intended. This can happen due to various factors, such as coding errors or bugs, or security vulnerabilities that are exploited by harmful attacks. Since smart-contracts can be executed on the Blockchain, there is no way to terminate them once they have been deployed (Krupa et al., 2021).

To prevent this issue, it is recommended that smart contract designers include a way to halt a vulnerable function or the entire contract in the event of a bug. Additionally, it is important for designers to thoroughly test their contracts in secure environments and to conduct thorough code reviews before releasing them for use.

Repudiation: Repudiation is the inability to deny making a statement, which is related to the security characteristic of non-repudiability (Zhou & Gollman, 1996). In the context of non-fungible tokens (NFTs), This means that the sender of an NFT cannot deny sending it, thanks to the security of the Blockchain and the inability to forge a signature scheme (Menezes et al., 2018). However, it is possible for a malicious attacker to tamper with the hash data associated with an NFT or to bind the hash data to their own address. To address this issue, we recommend using a multi-signature contract, which requires the confirmation of multiple parties for each binding (Wang et al., 2021).

2.1.2 Platform Related Challenges

Scalping Bots in marketplaces: One potential problem with NFTs is that they can be vulnerable to attacks by bots. Bots are automated programs that can be used to perform a variety of tasks, including buying, and selling assets on a platform. In the case of NFTs, bots can be used to manipulate the market and drive-up prices, or to scoop up valuable NFTs before other users have a chance to bid on them.

This can create a number of challenges for NFT platforms and their users. For example, the use of bots can lead for difficulties for users to exchange NFTs on a platform fairly and transparently. It can also create a perception of unfairness and mistrust among users, as some users may feel that the use of bots gives an unfair advantage to certain users or groups.

In addition to the potential financial impacts, the use of bots in the NFT market can also have broader implications for the industry. For example, it can contribute to market volatility and instability, which can impact the overall health and sustainability of the NFT market. It can also make it more difficult for users to trust the value and authenticity of NFTs, which could reduce the overall demand for NFTs and limit their potential use cases.

To mitigate this issue, there are a variety of bot detection and mitigation software solutions available that can help NFT platforms identify and prevent the use of bots on their platforms. These solutions typically use a combination of techniques, such as machine learning algorithms, user behavior analysis, and IP address tracking, to identify and block suspicious activity.

For example, a bot detection and mitigation software may use machine learning algorithms to analyze user behavior on the platform, such as the frequency and patterns of transactions, to identify anomalies and potential bot activity. The software may also use IP tracking to identify users who are accessing the platform from multiple locations or devices, which is a common tactic used by bots to avoid detection.

Once a bot is detected, the software can take a variety of actions to prevent it from continuing to operate on the platform, such as blocking the user's IP address, disabling their account, or issuing a warning to the user. Some software solutions may also include additional features, such as the ability to track and monitor bot activity over time, or to integrate with other security tools and systems.

Overall, using bot detection and mitigation software can help NFT platforms protect themselves and their users from the potential harm caused by bots, and ensure that their platforms are fair and transparent for all users.

Hardware Wallets Support: NFT functionality is typically included in modern hardware wallets. Nevertheless, there are some marketplaces that do not permit their customers to have direct access to these devices. It is either forbidden to do so or requires the use of a software wallet, both of which are cumbersome for the customers. They are required to carry out additional responsibilities, which may result in confusion or complications. Because of this, they are going to disregard using this method to store NFTs (Musienko, 2022).

The answer to this problem is as simple as ensuring that all popular hardware wallets that are capable of storing NFTs are supported by NFT platforms (marketplaces, video games, galleries, and so on). The well-known markets OpenSea, Rare, and SuperRare are all compatible with hardware wallets (Musienko, 2022).

Authentication policy: In the real world, it is not uncommon for works of art to be utilized in the process of money laundering. Since users can mint NFTs, this makes laundering a simpler task. In addition, they will not have to deal with the logistical challenges that are typically associated with transporting physical artwork. A significant number of cryptocurrency exchanges, such as Binance and Coinbase, have already implemented KYC and AML/CFT (Anti-money laundering, Combating the Financing of Terrorism). On the other hand, the marketplaces have not made any efforts to ensure compliance with KYC, AML, or CFT regulations (Musienko, 2022).

We recommend that NFT platforms to implement a comprehensive AML/CFT that outlines the platform’s compliance and to set out procedures to prevent money laundering, additionally, to conduct due diligence on customers and users of the platform to verify their identity and to check for red flags. We also recommend platforms to establish records and systems to track and monitor transactions and activities on the platform, to identify and report any suspicious activity

Market Decentralization: When NFTs are made available on the marketplace, they are moved to the trading platform's wallet. In this instance, the trading marketplace holds NFTs in escrow, which occurs off-chain. As a result, as soon as the seller transfers his NFT asset to the marketplace and till the exchange is finalized, the Blockchain is unaware of all transactions. This violates the decentralization principle and makes the purchase and sale of NFTs unsafe for all parties (Musienko, 2022). Escrows are a third-party smart contract. It holds the deposited tokens until the payment conditions are satisfied.

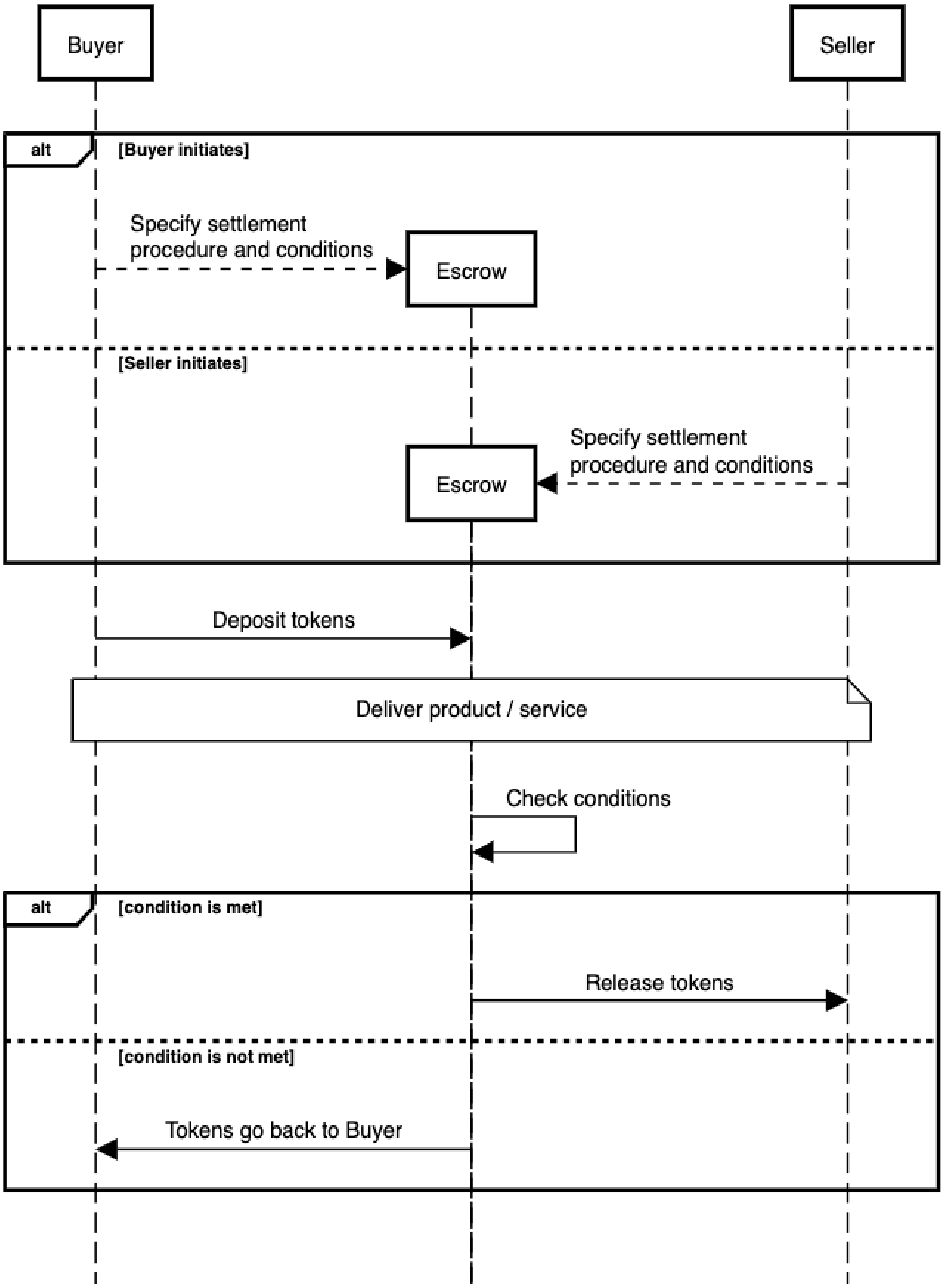


Figure 8. Escrow model diagram

Sources: (Lu et al., 2021)

If you want to ensure that your non-fungible tokens are safe, you should only use exchanges in which your private keys are not accessible and do not demand you to move the NFT to their wallet (how Nifty Gateway works). And for developers to create their NFT marketplaces in such a way that doesn’t go against the decentralization idea so that assets are not subjected to unnecessary risks.

Validation of entered information: The front-end components of the system are the NFTs applications, which engage with both the server and the smart-contracts The front-end, such as user-interface and the back-endare responsible for coordinating all aspects of the buying and selling process. Each parameter that is sent from the user through the interface needs to be validated after the application or smart-contract receives it. If it is ignored or put into place in the wrong way, it will cause negative effects or a loss of money (Musienko, 2022).

For instance, according to one of OpenSea's reports, a user intended to give an NFT as a gift but typed the recipient's nickname rather than their Ethereum address. This occurred when the user tried to send the NFT. Unfortunately, due to the fact that no one checked the correctness of the data before it was input, the NFT was either sent to the incorrect address or was misplaced.

It is important to make sure that the front-end and back-end of an NFT application are properly integrated and that input data is properly checked and validated. This can help prevent errors and ensure that NFT transactions are carried out smoothly and securely. It's also important for users to carefully check and verify the information they are entering, such as addresses and other details, to avoid making mistakes.

2.1.3 Users and Wallets Related Challenges

It was reported at the beginning of July that Bleeping Computer had discovered suspicious activity aimed at defrauding 2.3 million Bitcoin wallets, which they discovered were at risk of being compromised. This news came shortly after Bleeping Computer had discovered that these wallets were at risk of being compromised. Malware known as a "clipboard hijacker" was used by the attackers. This malware operates within the clipboard and has the ability to potentially replace a copied wallet address with one of the attackers' addresses (Rezaeighaleh & Zou, 2022).

As early as November of the previous year, researchers at Kaspersky Lab predicted the possibility of such hacking attacks, and it didn't take long for those predictions to come true. It is estimated that approximately 20 percent of all malware attacks are directed at individual accounts and wallets. This makes it one of the most common types of attacks that are conducted with the intention of stealing information or funds from users. Additionally, there is more. According to a report that was published by Coin Telegraph on July 12th, criminals were successful in stealing over $9 million worth of Ethereum (ETH) through social engineering schemes over the course of the previous year (Boireau, 2018).

The website Bleeping Computer, which promotes computer literacy, has an article about how important it is to follow at least a few basic rules to make sure there is enough security:

The majority of issues requiring technical support can be traced back to the user's lack of familiarity with the fundamental ideas that underlie all computing problems. This includes the computer's hardware, its operating system, its files and folders, the internet, and its applications.

The consensus view is shared by a large number of cryptocurrency experts. In a blog that is specifically dedicated to Hackernoon, one of the authors, investor and entrepreneur Ouriel Ohayon, places an emphasis on the individual responsibility of users. "You are responsible for your own safety, in addition to being in charge of your assets." In addition, the vast majority of people are not security experts, which means that they are frequently exposed without their knowledge. It never ceases to amaze me how many people, including those who are savvy with technology, do not practice even the most fundamental forms of security.

Lex Sokolin, the director of the fintech strategy department at Autonomous Research, says that every year, cloned websites and common phishing schemes trick thousands of people into sending out $200 million in cryptocurrency that they never get back.

It is well known that motivated opportunists pose a great danger to the safety and stability of any IT organization. These individuals attempt to rob any valuable digital or physical asset. They may even snatch chat messages. The NFT market is just beginning to expand, but its rapid capitalization growth and rising popularity have attracted many fraudsters and hackers.

We will now talk about challenges targeted against users and later possible solutions and how to mitigate being at risk.

2.1.3.1 Challenges and User Risks

Spoofing: Spoofing occurs when a cybercriminal assumes someone else's identity, or that of a corporation, in order to engage in malicious activities. The Spoofer could exploit a vulnerability flaw to obtain the original owner's private keys and then transfer the NFT to his wallet. The simple strong defense against this attack is to use a cold wallet in conjunction with formal NFT smart contract verification (Zhu, 2022).

Cold wallets, also known as cold storage, are secure, offline storage solutions that are used to protect NFTs from unauthorized access. They typically take the form of a USB drive (Jørgensen & Beck, 2022).

A NFT spoofing scheme could involve the creation of a replica of a reputable NFT store. Security Boulevard says that scammers make websites that look like the real ones and try to trick people into entering their login information or credit card information.

Creating a counterfeit NFT: The smart-contracts demonstrate the legitimacy of the NFTs. Before purchasing an NFT, we advise confirming the NFT address through official channels like the project's website. Sadly, users barely perform this action because they are unaware that it can be done. However, the users concentrate on the names and appearances of the lots on the marketplaces, enabling the criminals to offer counterfeit NFTs. Typically, fraudsters employ these techniques:

On the internet, there are numerous fake non-fungible tokens (NFTs) that mimic the appearance of legitimate collections or individual NFTs. These fraudulent tokens often use similar or identical names to those of legitimate NFTs, but they are able to evade detection by replacing ASCII characters in the original name with similar-looking, non-ASCII characters. For example, the Latin letter "C" could be swapped for the Cyrillic letter "C" without being noticed. This trick allows these fake NFTs to pass as genuine and potentially deceive unsuspecting buyers.

To combat this type of fraud, OpenSea has implemented measures to prevent users from using commonly used collection names or specific special letters and symbols in their NFT listings. However, users can still attempt to circumvent these measures by having a period (.) to a name’s ending or changing the case of letters. For example, a user might rename the collection "CryptoWizards" to "Cryptowizards" in order to bypass the restrictions. It is important for users to be vigilant and carefully make sure the NFT is genuinely prior of making the purchase to avoid falling victim to these types of scams.

Each image has a unique URL address, but they all point to the same location. There have been instances of fraudulent NFTs that copied the image URL of legitimate NFT assets. Fraud actor can, for instance, release smart-contract and mint tokens that resemble a common collection, such as CryptoPunks. These are both easy targets for cybercriminals. It is possible for the customer to mistake these NFTs for genuine items if the customer focuses only on the item's surface appearance and does not investigate its authenticity.

Unfortunately, it can be difficult to protect yourself from this type of fraud as there are currently few reliable ways to verify the authenticity of an NFT or the identity of the person selling it. Unless the NFT is being sold by a well-known celebrity or a widely recognized token. One possible way to enhance security in this situation is to implement a reputation system and vendor verification mechanisms, such as a Know Your Customer (KYC) procedure, to help identify and authenticate legitimate sellers. While these measures may not completely eliminate the risk of fraud, they can help to reduce the chances of falling victim to a scam.

Similar images. The creation of a fake NFT can also be accomplished by copying a virtual asset (image, clip, or track) and minting an NFT that directs to the copy of the virtual asset. Because of how easy and accessible it is, this type of fraudulent activity is quite common in the market for NFTs. There are many tokens on platforms that make it possible to generate NFTs with no required cost.

No marketplace conducts NFT comparisons inspects to verify whether a file has previously been used in other NFTs. These checks are necessary in order to answer the following question: Because of this, it is the responsibility of each user to conduct these kinds of checks by using Google or other tools to locate content that is comparable to what they are looking for.

Social Engineering (Phishing): It is not uncommon to be able to recognize a variety of psychological manipulations that are designed to coerce the user into carrying out specific actions or divulging private information. Fraudsters can obtain funds, login credentials, credit cards, confidential information, and other personal information through the following methods, which do not involve hacking into the individuals' computers or mobile devices: Social engineering, in contrast to more traditional cons, calls for a significant amount of planning and preparation.

Spear phishing, the most common form of phishing, the fraudster needs to create an email as well as a website or application to which the email will lead. It will assist in retrieving the login credentials for the user.

Other ways available. Frequently, fraudulent activity will involve the development of phony applications that pretend to be well-known wallets, exchanges, or marketplaces. These fabricated applications frequently sail through Google Play and the App Store's verification processes.

Installing software that secretly records keystrokes or contains viruses is an additional method of phishing. The con artist will typically make contact with the victim through social media or instant messaging applications and convince him to download and extract a compressed file that is password-protected. Virus scanning is prevented from accessing the contents of the compressed file because it is password-protected. When the victim extracts the file and starts the installation of the harmful software, the system will be infected with malicious code as soon as the victim has completed both of these steps. For example, the malicious actor is able to obtain the victim's username and password whenever the victim launches a wallet using Metamask. The hacker (or hackers) can steal all user tokens if they have this information as well as the original seed phrase which is also known as user phrase, which is saved on your computer. If the wallet is connected to a bank card, these funds will also be taken from the card.

2.1.3.2 Possible User Security Solutions

Multi-Factor Authentication (MFA): To gain access to an application or website, a user must provide multiple types of verification, such as codes or factors, to the authentication system. Once these have been successfully presented, the user is granted access.

If multi-factor authentication (MFA) is not in place, a hacker can easily compromise an NFT account. MFA can mitigate cybercriminal attacks because it stops unauthorized parties from having access to the users' information (Kinyua, 2022).

Strong Passwords: Large technology corporates illustrate why unique and strong password is needed. Strong, unique, and easily-remembered passwords are required for accessing NFT websites. For example, use special characters, capital letters, lowercase letters, and a combination of digits to create a unique and secure password. Do not use two or more passwords that share most of their characteristics of NFT or any website.

For example, using a password like makes it easier for hackers to try and guess or brute-force the password, and it also makes it more likely that all of these passwords will be compromised if even one of them is compromised. Have your password on a written on a piece of paper instead of relying on a website that allows you to retrieve lost passwords. It will make it easier for you to keep your NFTs and cryptocurrency wallets safe.

It would help if you had a unique password that was long enough and hard to guess especially when it's used with a multi-factor authentication. Best of all, it should be a random set of numbers and symbols made by a program like Google Chrome that makes hard passwords for you when you sign up for something (Kinyua, 2022).

Avoid cold emails and suspicious downloads: Everyone has received an email advertising a business or a file. Since they are unsolicited, the emails often appear too good to be true. Avoid opening emails sent by random people, as this is one of the more known ways to contain malicious soft wares. It could lead to a malicious person stealing your credentials, compromising your account later by stealing your NFT or identity (Kinyua, 2022).

Regularly update your software: With time, the outlook for NFTs improves, but so do security challenges. Users must sure that the NFT software runs smoothly by consistently patching the most recent version available for your device. After installing the new update, it will fix any software driver bugs. As a result, it reduces the number of potential attacks.

Secure internet connection: Ensuring the security of your home internet connection is crucial for protecting yourself from online dangers and using the internet with peace of mind. It reduces the likelihood of hackers gaining access to your NFT accounts and hardware wallets.

Store the backup phrase in a safe place: It is extremely advisable not to keep your wallet's seed phrase in a digital file. You can't use your smartphone to take photos, turn them into text files, or save them on your hard drive. It would help if you didn't put it in an app that stores passwords, it can be hacked or broken into, which would cause NFTs to be lost.

An effective solution is to utilize a paper or titanium drive (such as CryptoTag.io) in conjunction with the RAID storage method. The concept is to distribute data across three separate drives. For example, if a file is divided into three parts, the first part would be stored on the first drive, the second on the second drive, and the third on the third drive. To securely store a seed phrase, it is recommended to shuffle the words and spread them out over multiple pieces of paper.

Regularly Back Up Your Wallet: Thus, in case of a system failure or a device loss you can always recover your data. It is advisable to make multiple backups, and have the data on three or five drives simultaneously, with one or two external hard drives that are not connected to a computer or the Internet. This will best protect your NFTs.

Regularly update your software: In any case, updating your software is important. Some patches are made for security concerns and to patch vulnerabilities if they exist. Either set your wallet, antivirus, operating system, and email client to update themselves automatically or manually check for patch updates when possible (Kinyua, 2022).

Use a secure connection to the internet: When you use an open Wi-Fi (eg., public café's Wi-Fi), hackers find it much simpler to access your data. If you have to connect to an open network, use a VPN to keep your data from being encrypted by other apps. Also, turn off the visibility and Bluetooth on your device.

2.2 Privacy Challenges

The level of anonymity and privacy offered by NFTs is not well understood. Most NFT transactions take place on the Ethereum platform, which offers pseudo-anonymity but not complete anonymity or privacy (Wang et al., 2020). Users can keep their identities partially hidden if the public is unaware of the relationship between their true identities and associated addresses. However, all user activity associated with the disclosed address is visible. Currently, privacy-enhancing solutions such as homomorphic encryption (Wang et al., 2020), zero-knowledge proof, ring signature (Noether, 2015), and multi-party computation (Raman et al., 2018) have not been applied to NFT schemes due to the complexity and security assumptions of their cryptographic primitives. As with other Blockchain-based systems, the challenge of implementing privacy-ensured methods lies in reducing high computing costs.

In a survey done by the digital security company Privacy HQ, 90% of people said they had been a victim of some scam, 50% said they had lost access to their NFTs at some point, and 65% said they had sold out of fear in the past.

Since mobile devices are portable, easily lost, and frequently connected to public Wi-Fi, mobile banking tends to be less secure, prompting most respondents to opt for desktop computers. 10% of NFT owners polled have thus far avoided fraud. (NFT Security Concerns - Fintech News)

NFTs are unique and easy to identify by nature, which makes them non-fungible and desirable to a subset of Internet users. In Web 3.0 and the so-called "emerging Metaverse," it's becoming more common for people to make online avatars or profile pictures (called "PFPs") and create a digital identity that is either based on their real selves or is completely different from them. As part of their online presence, people who use Twitter, Instagram, or online messaging apps may use a PFP.

If a PFP or avatar can be used to find out who someone is, it might be considered personal data or information. In most cases, though, a PFP or avatar will only show a pseudonymous online identity that was made on purpose to be separate from the real person behind that online identity and inaccessible to that person. There are two concerns about this:

First of all, most users can't be sure that a digital trail won't be able to link their online identifier (and, by extension, their whole anonymous online life) to their real identity.

Second, the idea of linking personal information to a person may become outdated in the near future if (or when) millions of people have sophisticated online identities with social and economic value. Don't assume that existing privacy laws don't apply to online identities, including those based on NFTs. This is a fundamental problem that lawmakers and policymakers will need to solve at some point.

Cryptographic assets are saved on the Blockchain at a specific address and can be accessed through a wallet, which lets users send and receive assets to and from their address. The things in cryptocurrency wallets can be seen by anyone.

On the Blockchain, each address is unique. Most NFTs are stored and traded on the Ethereum network, where the addresses are usually a random string of 42 hexadecimal letters and numbers. But more and more people who own crypto assets link their wallet to a ".eth" domain, which is also called an Ethereum Naming Service ("ENS") domain.

Even though cryptowallets are usually associated with privacy, many wallets with an ENS domain will show who the user is (or what their online name is). This can be done directly if their ENS address is their name, like AhmadAli.eth, or indirectly by referring to their Web 3.0 identity, like gamer1234.eth, which may or may not give away the person's real name.

Also, it is possible to see all of a user's assets and transactions in their wallet, even if their wallet doesn't use an ENS domain. By using information that is available to the public, this may give hints about who owns the wallet. If there is a public record of the person owning or trading a single NFT or if they have made their wallet address public, the wallet and its contents are tied to the person and their crypto assets are made public.

A company has two options, either to establish their own wallet or have a third-party manage its digital assets to release an NFT or receive sales in crypto. The company should determine which customers will open their wallets as part of this procedure. In addition, since the employee may have privacy rights, the company should link their wallets it makes to a company account instead of the employee's account (Musamih et al., 2022).

A company must think about how to protect the private keys of the wallet, which are the safe's passcode. Digital wallets are only as safe as the user's private key, which is also called the "seed phrase," "secret phrase," or "recovery phrase." Anyone could steal a seed phrase that is stored online, on a computer, or in an electronic password manager. Once a bad actor gets a brand's seed phrase, they can move its digital assets to a wallet they don't control. Because of how Blockchain technology works, these transactions cannot be taken back.

Brands should be aware of the ways that bad people get into digital wallets. Most attackers get into online accounts by phishing, which leads them to a digital wallet in the end. Attacks are especially likely to happen on Twitter, Instagram, and Discord. An attacker gains access to an NFT issuer's Discord, Twitter, or Instagram account, tweets, or posts about a new NFT drop along with a malicious link, and then gains access to the private keys of users who click on the link (either through a vulnerability on the user's device or as part of a bet to connect their wallet to the attacker's website). At least once, an attacker got into an iCloud account and found that his seed phrase was stored in the backup data. Millions of dollars’ worth of assets and cryptocurrencies have been stolen from the people who fell for these scams. Also, when a brand is attacked, it can face a lot of legal trouble and damage to its reputation (Uribe & Waters, 2020).

Therefore, brands must take the necessary precautions to prevent such attacks and respond swiftly. Even simple steps like training employees and limiting access based on "need-to-know" protect the brand and any NFT buyers interacting with it.

When discontinuing an NFT collection, there are numerous factors to consider, with privacy and data protection compliance being the most crucial. Failure to address privacy and data protection could increase regulatory scrutiny and enforcement, harm consumer confidence, and goodwill, and result in valuable assets and revenue loss. In addition, as Web 3.0 gets closer, best practices and laws will change, and brands must stay up-to-date and flexible to meet their obligations (Babel et al., 2022).

Leakage of information is another privacy concern that arises when data is available to unpermitted individuals. In the NFT system, information related to status and smart contract procedures are transparent, meaning that any state changes are visible to any observer. This means that even if a user simply looks up an NFT hash on the Blockchain, malicious attackers can potentially access and abuse the information and transaction history associated with it. This vulnerability exposes users to the risk of having their data accessed or exploited by unauthorized parties (Ali et al., 2022).

An NFT's Information could be leaked if they are stored on platforms that are not secure or are not encrypted, if NFTs or their metadata are shared on public platforms or if third parties get access to or share information without permission (Ali et al., 2022).

Because of this, we urge the developer of the NFT to use complex contracts and secure storage platforms that protect the user's privacy instead of simple, smart contracts.

2.2.1 Secret NFTs

A Secret NFT (Non-Fungible Token) is a digital asset that is stored in a Blockchain, similar to traditional NFTs. However, unlike traditional NFTs, the ownership and value of a Secret NFT can be kept private, as the creator has the option to make the file and metadata (such as the price and owner) visible only to themselves and the purchaser. This allows the creator to maintain a level of secrecy and control over the NFT, while still benefiting from the security and immutability of the Blockchain. Secret NFTs can be utilized to portray a variety of assets, including art, music, video, and other forms of media. They offer a way for creators to protect the privacy of their works and the ownership and value of their NFTs, while still taking advantage of the benefits of the NFT ecosystem.

Secret NFTs have numerous applications. Because of the privacy feature, art galleries can keep some pieces of work to themselves. Without disclosing their financial information and NFT assets on the public Blockchain, art lovers can own works of art discreetly. Additionally, it permits sealed art bidding so that buyers may be confident that their financial situation won't affect the price. (Scrt Labs, 2022)

Additionally, secret NFTs open up additional opportunities for the inventor. Content might be watermarked or marked as sensitive by the artist. They can also establish private exhibits that are only accessible to NFT owners by setting a password in the metadata or sharing unique information with NFT customers.

Secret NFTs enable the protection of identifying information on event tickets or tokens outside of the realm of the arts. Real estate investors can transfer ownership history between parties without making it publicly known thanks to the privacy function. Secret NFTs can be used in games to keep players' assets concealed from rivals, to activate hidden skills after a specified amount of time, and in games that rely on secrecy to disguise players' actions. (Hoory, 2022)

The biggest creators in the world are using secret NFTs to distribute their work. In partnership with SCRT Labs (Secret Network), the original core development team behind the Secret Network, Quentin Tarantino launched the Tarantino NFT collection.

The handwritten original screenplay for Pulp Fiction, which has remained secret since the movie's 1994 debut, was transformed into Secret NFTs by Tarantino. He published a number of NFTs as part of a collection, and each one "consists of the original script from a single classic scene, as well as individualized audio commentary from Quentin Tarantino himself." (Hoory, 2022).

2.3 Other Challenge

Environmental Challenges: The energy consumption of Bitcoin and Ethereum transactions is a cause for concern. A single Bitcoin transaction consumes approximately 926.23 kWh, the amount of electricity consumed in a single month by the average American household (Digiconomist, 2021). A single transaction on the Ethereum Blockchain consumes an average of 74.79 kWh, or the energy equivalent of 2.5 days (Digiconomist, 2021). These high energy demands are largely due to their validation method, which relies on solving complex computational problems for the purpose of expanding the chain by adding new blocks. Miners with stronger computers have a bigger opportunity of receiving cryptocurrency or network fees, leading to a race for more powerful processors and higher energy absorption. Right now, most NFT marketplaces use Ethereum’s Blockchain to create new blocks and adding them to the chain (Barber, 2021). However, as Ethereum evolves into Ethereum 2.0, it is expected to shift from proof-of-work to proof-of-stake, which is considered more environmentally friendly (Vashchuk & Shuwar, 2018). Proof-of-stake can verify transactions without requiring to solve intensive mathematical problems, making the it more environment friendly. While the switch to proof-of-stake has been discussed since 2017, Now there exists several different Blockchains which use it while having a smaller carbon emission than Ethereum, such as the Tezos Blockchain.

Gas Fee - On the Ethereum Blockchain, all transactions incur a variable fee known as the "gas fee". Miners who validate transactions on the Blockchain are rewarded with the gas fee. It is sent from the sender to the miner's address as the transaction fee. "Proof of work" is a common method used in numerous Blockchains. The fee for gas is measured in "gwei." One gwei is 0.000000001 ETH (Kasireddy, 2017). The price of gas fees fluctuates based on the network's congestion and the price of Ethereum. As depicted in the graph below, gas prices are typically lowest on weekends, when fees are the lowest.

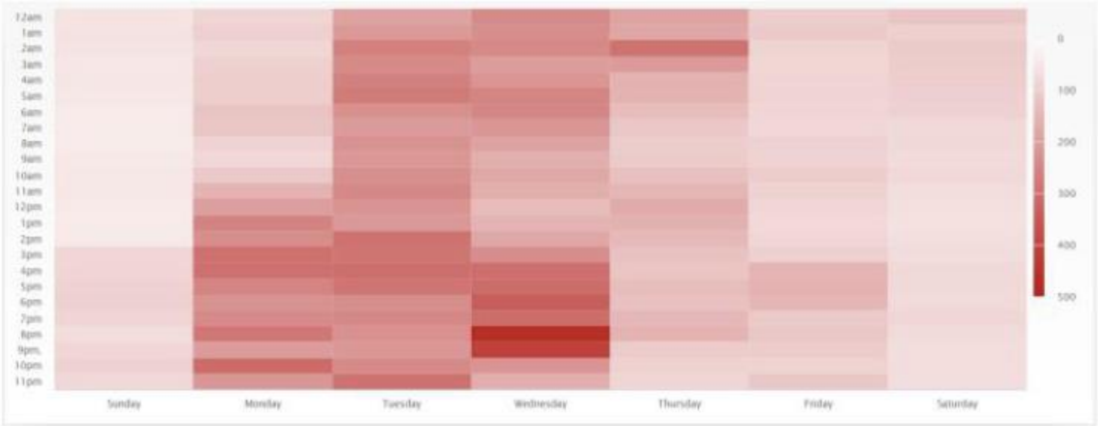


Figure 9. Gas Price by Time of Day

Source: (El Faqir, 2021)

One of the challenges facing NFTs is the variable gas fee price on the Ethereum Blockchain, which can be a problem, mianly for low-cost NFTs that may not be able to afford the high fees. To address this issue, alternative Blockchains such as Cardano or Polkadot, or a future version of Ethereum 2.0, may be a better option for minting NFTs.

Extensibility issues - One of the most important things about NFTs is that they can be combined with other NFTs to make new, unique NFTs. The fact that NFTs are extensible is both advantageous and problematic. The problem of extensibility centers on two main points: NFT interoperability and NFTs that can be upgraded. Existing NFT ecosystems are siloed, and NFTs within an ecosystem can only trade with other NFTs operating in the same ecosystem or network. You just need to talk to people outside of the chain to make it happen. Since most NFTs are currently deployed on the Ethereum Blockchain, their scalability has not been tested and is assumed to be fine. It may become even more crucial in the future, however, as new NFT and Blockchain technologies such as Cardano and Polkadot emerge (Wang, 2021).

Soft forks: Blockchain networks often undergo updates in the form of minor modifications that are compatible with previous protocols (minor forks) and significant changes that may not be compatible with previous protocols (hard forks) during their development. These updates can cause conflicts for NFTs (Wang, 2021).

Art Theft: Art Theft is a major weakness in the NFT system. A malicious actor can steal another user's NFT that has not yet been uploaded to the Blockchain and convert it to an NFT in an attempt to assert ownership

Processing Time: When creating or trading NFTs, smart contract is used to transfer NFTs, that requires contact with the Blockchain. As of now, the Blockchain transaction process takes a long time, resulting in poor user interaction. But there exists few proof-of-stake (PoS) Blockchains, such as Algor, that have partially addressed this issue, but there is still much work to be done.

Anonymity: Most NFT projects today are built on Ethereum, Flow, or Tezos, but none of these offers full anonymity to their users. Since everyone can see the balance and transactions associated with a given wallet address, they provide only a veneer of privacy. Bad actors like hackers can use this data to break into some wallets. Most Blockchains have yet to adopt techniques such as zero-knowledge proofs and multi-party signatures, despite their obvious utility.

Legal issues: Numerous NFT exchanges lack a KYC (know your customer) policy, as has been observed. Before investing in space, it is essential to comprehend a country's regulatory framework due to the fact that it involves commodity trade and even cross-border activities. In addition, because the sale of NFTs is not currently considered a taxable event, this could lead to widespread financial fraud. Consequently, governments should consider taxing and regulating in order to protect their citizens.

Storing NFT off-chain: Since storing a photo or clip file can lead to a need of a huge amount resources, resulting in a high gas fee that may lead to the congestion of network, most NFT marketplaces store digital art in non-Blockchain databases. As a result, the token is identified on the Blockchain using a simple cryptographic hash.

3. USE CASES AND APPLICATIONS OF NFT

Listed under this section are some of the various NFTS use cases, as well as examples of common applications of NFTS.

3.1 Use Cases

3.1.1 Gaming

The gaming industry and NFTs are very compatible technology. By allowing cross-platform play, NFTs could be implemented and used in the gaming sector. Players who have characters and items in a video game will almost certainly keep playing it. NFTs provide video game makers with an additional way to build their brand and generate income (Bernstein, 2021).

Since the rarity of NFT in-game items and variation, trading can be facilitated in the NFTs games. Which could lead to a new economy for players, for example you can trade a very rare NFT item and sell it to the highest bidder. Due to the lack of a middleman and the instantaneous nature of Blockchain transactions, NFT owners will not be vulnerable to fraud.

This opens up many opportunities, being able to purchase firearms and other tools which actual users had tested before is an example. This application has already begun to be fully utilized by future Blockchain games.

3.1.2 Real Estate

NFTs is utilized to seamlessly to transfer land deeds, establish title ship, and track changes in property value when applied to real estate and ETFs. The timestamped nature of NFTs allows for a clear record of these transactions and makes them a valuable tool in the real estate industry. Together, NFTs and real estate can be a powerful combination for managing and tracking property ownership and value.

When compared to other industries, real estate is well-prepared to use NFT. Protecting private information like credit card numbers, NFTs can be used in the real estate sector to streamline and speed up transactions, Smart contracts can be utilized to facilitate automated payments for properties, and decentralized platforms for house rentals can be created. Just picture yourself being able to get any and all information you need about the house you're looking to buy by simply tapping your phone. Before buying a home, it's important to do thorough research into the building's history, including its initial construction date, its previous owners, any renovations that have been done, and more (Bernstein, 2021).

3.1.3 Voting

In order to cast a ballot, voters are typically required to bring a photo identification along with them to the polling place, as well as evidence that they reside in the district. On the other hand, a significant number of people are unable to vote due to the lack of possession of a valid identification document, extra proof of address, or aren't registered to vote.

Because NFTs would provide individuals without physical identification that demonstrates who they are and where they reside in the country with a digital identity, they can help find a solution to this problem. This is because a person's physical ID shows who they are and where they live in the country.

This can cut down on election cheating and fraud because NFTs can be used as an official record of voters and their votes.

Additionally, this can increase the transparency of many transactions, primarily by confirming who owns tangible assets such as real estate, ideas, artwork, and others. Over the next few years, more progress will be made in this area, and at the current rate, it may have already occurred (Bernstein, 2021).

3.1.4 Medical Records and Identity Verification

Every record in the Blockchain is verifiable and resistant to any malicious efforts to tamper with it, as NFT transactions are checked by multiple nodes before they are permanently recorded on the Blockchain.
Therefore, the NFT chain can be used to have a person's medical records in a way that does not expose them to the probability of being viewed by a non-authorized people or put them at risk of being altered by a third party.

An example of NFT applications that have been designed to aid medical professionals include the creation of NFT birth certificates, which doctors and nurses can provide to newborns.

It might be simple to link a person's birth certificate to their permanent identity on the Blockchain if that person was given one of these NFTs when they were born. After that, an independent verification of this identity could be carried out utilizing NFT validation applications. NFT chains are safe to keep personal health information while still letting medical professionals like doctors and nurses get to it when they need to. NFTs now have narrowly defined applications, and hospitals, health insurance companies, and other groups are looking into how Blockchains could improve hospital operations by validating patient records and keeping track of medical procedures while keeping patient privacy safe. (Bernstein, 2021).

3.2 Applications

3.2.1 The Metaverse

The Metaverse is a hub many users go to and interact with each other in a way that is both real and digital. "Post-reality universe" is another name for it. It is built on the fusion of technologies like virtual reality (VR) and augmented reality (AR), which enable users to interact with virtual environments, digital objects, and other users using all of human senses (AR). So, Metaverse can be a social hub, inter-connected, true to life landscape that are hosted on platforms that can be used by more than one person and that stay the same. It lets people talk to each other in real time while interacting with digital objects. In the first version, avatars could move from one virtual world to another by teleporting. In the latest version of Metaverse, there are Virtual Reality (VR) platforms which are used to socialize in a close-to-life environment that work with video games, and collaborative spaces that use Augmented Reality (AR) (Mystakidis, 2022).

Computer science's progress has a big impact on everyday life because it changes and improves how people interact, communicate, and do business with each other. From the point of view of end users, there have been three major waves of technological innovation, each centered around a different disruptive innovation catalyst: the introduction of computers, the web, and smartphones. Virtual reality (VR) and augmented reality (AR) are examples of innovation that are a front leader in the coming fourth computing industry wave, which is happening right now (Kamenov, 2017). It is anticipated that the adoption of Blockchain technology will result in a shift towards "pervasive computing," which has the potential to transform industries such as education, business, remote work, and entertainment. This new perspective is referred to as the "Metaverse".

The term "Metaverse" is a neologism, comprising the Greek prefix "meta," meaning "after" or "beyond," and "universe." In this context, the Metaverse refers to a virtual realm that exists beyond our physical world. It is a place where people are always doing things and where many people live. It is a mix of real life and digital simulation. Metaverse may be able to fix the main problems with web-based 2D e-learning tools, which would make it possible for the platform to be used for online distance education.

Extended reality, also called "cross reality" (XR), is term for a group of software innovations that make you feel like you are in a different place. These technologies make digital and electronic environments where data can be shown and represented. Extended reality (XR) includes virtual reality (VR), augmented reality (AR), and mixed reality (MR) (Milgram et al., 1995). All of the above uses of extended reality (XR) involve people watching and interacting in a digital environment that was made by technology, either completely or in part.

Both the business world and the academic world have been paying a lot of attention to the latest buzzword, which is "Metaverse." Both real and virtual worlds are brought together by utilizing Metaverse technology, which also enables avatars (online personas) to participate in a wide many different events, like creating, displaying, entertaining, social media, and conducting business. Exploring the Metaverse offers the opportunity to create a dynamic digital world and make the real world a better place. This presents a very promising outcome.

In this chapter we will talk about the Metaverse. Specifically, we discuss how non-fungible tokens (NFTs) combine with the Metaverse. Collaboration from both academic institutions and private businesses will unquestionably be necessary in order to further exploit and conduct scientific study of NFT fusion in the direction of the Metaverse.

The rate at which technological progress affects human lives is accelerating at an increasingly rapid rate. The fusion of virtual reality (VR) and physical reality in an online environment is what is referred to as the "Metaverse," also called as the three-dimensional internet. With NFTs serving as the primary structural components of the new extensive virtual ecosystem, it is possible to alter the internet as it is known of today. This fully immersive, third-dimensional virtual world has many of the same characteristics as the world we live in, in addition to added capability of altering the environment to suit the specific wants and needs of each user (Usmani et al., 2022).

In the Metaverse world, non-fungible tokens (NFTs) may be an important role in the ecosystem. The use of NFTs for the transaction of virtual property could become more widespread if NFT Metaverse initiatives were implemented (Weston, 2022). Users can root and show their support for a certain football club or simply demonstrate their thoughts and opinions by purchasing NFTs. Because of this, NFT owners whose tastes are similar to each other could get in touch with each other and form communities where they could talk, share ideas, and work together.

In the early 1990s, sci-fi author Neal Stephenson first mentioned the Metaverse in his novel Snow Crash (Joshua, 2017). In recent years, as technology has advanced significantly in areas such as Blockchain, the Internet of Things, Virtual and Augmented Reality, Artificial Intelligence, Cloud and Edge Computing, the term Metaverse has gained significant attention in the tech industry. Roblox, a popular sandbox game platform, was the first company to include the word Metaverse in their publications and outline main attributes such as identity, social connections, immersive experience, ease of use, social norms, economy, accessibility, and variety as defining features of Metaverses.

Facebook, a social networking corporate, will change its name to Meta (Meta, 2021) in order to aid in the creation of the Metaverse and enable people to meet one another, learn from one another, work together, and have fun in ways that are beyond their ability to imagine. The video game Fortnite (Epic, 2017) by Epic Games release is also joining into the virtual world, game events such as a zombie world, where they can experience new levels of photorealistic interaction (Ambrasait, 2021; Epic, 2021; Seymour et al., 2017) and watch virtual concert performances (Kain, 2021).

Avatars are given the ability to participate in a different variety of rich events thanks to Metaverse's seamless convergence of both real and virtual worlds. These activities include creating, displaying, entertaining, socializing, and trading. Exploring the Metaverse is becoming increasingly popular in both business and academia. For instance, Jingteng Tech (Tech, 2022) has developed Beam Link, a platform that enables users to collaborate on interactive meetings, share photos and documents, and communicate with one another. In addition, the photo detection devices, such as depth sensors and camera systems, that are used in conjunction with CNNs are frequently put to use for the purpose of capturing dancers' motions and movements. The poses and movements of dancers can be used to create a three-dimensional feature space. This space can then be translated into dance performances in virtual worlds (Aristidou et al., 2019) using techniques such as dynamic time wrapping (Ferguson et al., 2014). Autonomous avatars, in contrast to the physical world, are able to comprehend the voice-to-motion mapping performed by human dancers. Because of machine learning, characters in Metaverse can imitate dance moves with a significant degree of correlation to the original dance, as well as emotional expressions.

The researchers have a problem in that they are unable to properly assess the shape and limits of the future Metaverse, which is problematic given the potential of the Metaverse. They could only think of a few of its possible features, like open space, decentralization, the experience of interacting with a computer, digital assets, and a digital economy.

In the Metaverse, human players' avatars, creations, and the things they use all have real-world effects. These things can even change the way people act in the real world by changing the way they think (e.g., how they choose to spend their leisure time). This change has big effects on society as a whole (Lee et al., 2021; Dionisio et al., 2013). As a result, it changes the way people live in a post-human society and rebuilds the digital economy at the same time. The Metaverse can be thought of as a fully functional and self-sustaining economy, as well as a full chain for making and using digital goods. The "economy of the Metaverse" is the way that people in the digital world act in terms of production-based economics. For example, the most important parts of the digital economy that happen in the digital world are creation, exchange, and consumption.

The integration of Blockchain technology and artificial intelligence and the Metaverse presents several new challenges to study, even though the introduction of Blockchain and AI has resulted in the development of enormous number of innovative technologies and applications. For instance, due to the characteristics of digital goods and markets, the volume of transactions that take place in Metaverse systems is significantly higher than what is seen in the real world. Non-Fungible Tokens (NFTs) enable avatars to create and content using digital certificates powered by Blockchain technology (Nadini et al., 2021; Lambert, 2021).

3.2.1.1 Understanding the Relationship Between NFTs and the Metaverse

Nearly all of the conversations revolving around the Metaverse are pointing towards the possibilities of combining the Metaverse with non-fictional worlds (NFTs). At the same time, many individuals have the misconception that non-fungible tokens are merely an additional component of the overall Metaverse. In fact, you will discover that NFTs and the Metaverse are considered to be virtually interchangeable versions of the same thing.

The most important factor that contributes to such presumptions is the rapid expansion of the use of NFTs in gaming, which is powered by Blockchain technology. It is reasonable to infer that only through the medium of virtual worlds will the Metaverse take shape. By providing a service to the various virtual worlds, interoperable Metaverse games have the potential to propel the development of the Metaverse.

A fully operational Metaverse is not going to be visible to the general public for at least a few more years. On the other hand, numerous Metaverse platforms have already established a name for themselves in the Web 3.0 ecosystem as a result of the distinctive functionalities that they offer. The gaming industry is currently home to the majority of the Metaverse's use cases, which can be observed today. When you can identify the fundamental connection that exists between the two concepts, the distinction between NFT and the Metaverse might become a little bit clearer to you. Tokens or products that are not fungible are absolutely necessary in order to engage in commercial activity within the Metaverse. Within the Metaverse, NFTs act as representatives of asset ownership for their respective owners. For example, virtual land parcels are actually NFTs.

The numerous possibilities that come along with the combination of NFT and the Metaverse would completely alter the future. You can see how non-fungible tokens (NFTs) bring ownership and uniqueness to the table, while the Metaverse provides a digital world in which anything is possible. The merging of the digital world with a system that can accurately represent both physical and digital assets in the physical world would bring about profound shifts in the economy as well as in people's social experiences. Even though many people believe that non-fungible tokens (NFTs) are already a part of the Metaverse and others believe that NFTs are the fundamental components of the Metaverse, it is abundantly clear that the combination of NFTs and the Metaverse would make a wide variety of new opportunities available.

Additionally, the association of identities from real life with digital avatars opens up opportunities for defining access to the Metaverse through the use of NFTs. 2019 marked the year in which the first instance of NFT-controlled access became visible. This event served as a prime example of the Metaverse NFT token. In 2019, the very first NFT.NYC conference required attendees to have an NFT-based ticket in order to gain access to the event. Even if no one could call the conference a "Metaverse," it undoubtedly established a model for how the NFT Metaverse should interact with one another.

In recent times, a large number of new projects have emerged with the aim of capitalizing on the intersection of NFTs and the Metaverse. A promising benchmark has been established. The projects are primarily centered on the introduction of significant paradigm shifts in the methods for conducting interactions online. The use of LAND tokens, as seen in the case of Decentraland, demonstrates how users can acquire ownership of real estate in the Metaverse.

The Metaverse is a vast idea, and non-fungible tokens (NFTs) have the potential to play an important role in the larger ecosystem. The use of NFTs as a virtual property deed could become more feasible as a result of projects involving NFT Metaverses. NFTs could be helpful in gaining exclusive access to enter a location in the Metaverse while also allowing others access to the location.

It is interesting to note that the smart contract functionalities that are included in the NFT could also be of assistance in the process of selling real estate on the Metaverse. When the Metaverse was first being developed, the use cases for NFT focused their attention primarily on NFT's capacity to control access to the Metaverse. In the same way that the first-ever real-world example of implementing NFTs in the Metaverse was able to help ensure VIP access to events in the real world, so too could NFT-controlled access help ensure VIP access to events in the Metaverse. Therefore, it should come as no surprise that the Metaverse and NFTs are a perfect match for one another.

3.2.1.2 The Role of NFTs in the Development of the Metaverse

Currently, the primary contributors to the economy of the Metaverse are land development and leasing, game task rewards, and profits from investing in cryptocurrency, and the bidding of virtual objects (eg., land, collectible items). As a result, the Metaverse gives rise to a novel method of funding that takes its cues from both the real world and the virtual world. NFT has been utilized primarily for the purpose of commemorating significant events or collecting digital assets; however, as of late, it has been utilized to create a new digital content business by combining itself with Metaverse (Capital, 2021). By storing an encrypted record of all previous transactions in perpetuity on the Blockchain, NFT is able to ensure that the digital assets in question are one of a kind. Each token has its own distinct value that can be easily identified, which makes it possible to verify the ownership of digital items. For instance, the NFT that is powered by Blockchain has been utilized to demonstrate the one-of-a-kind nature of both the avatar and the things that have been created in the Metaverse (Jeon et al., 2022).

And this is why there has been a shift toward the concept of a Metaverse that is founded on crypto assets. A kind of physical nature can be attributed to crypto, just as it can be attributed to the world. A Bitcoin or an NFT cannot be replicated in any way. In the same way that the glass of water on a desk can't take up the same amount of space as the glass sitting next to it. The space itself is unique and unchangeable, also it is not possible to make a copy of it. Even if you make a replica of the glass using 3D printing, it won't be the same glass. Therefore, cryptography is ideally suited for the construction of an immutable layer that describes the world as it is. Within the realm of cryptography, it is possible to construct representations of a real-world object that retain many of the characteristics which the real world has.

The digital equivalents of physical objects will present the most obvious opportunity. The physical world is inextricably linked to the information that is generated by digital twins, which can be used to model buildings or other physical assets. To put it another way, digital twins can be used to represent physical objects or spaces in the virtual world. They can be linked to Blockchain technology through the use of non-fungible tokens (NFTs), which can be used to verify and track the ownership and transaction history of the digital twin. Digital twins in the Metaverse can be used to create immersive and interactive experiences that bridge the real and virtual worlds.

It is of extreme importance to keep in mind that verification and validation are at the heart of crypto when attempting to assess the relationship between crypto and Blockchain and the Metaverse. When thinking about the relationship between Blockchain and the Metaverse, it is logical to think of Blockchain as a verifiable virtual realm.

One aspect that sets NFTs apart from other virtual tokens is their connection to the validation and verification process over time. This characteristic is what makes NFTs non-fungible, or unable to be replaced or exchanged for something else of equal value, this also means that copies of NFTs are impossible to create. Now link that with the Metaverse world.

This concept is revolving heavily around NFT domains. They become an immutable data space that is inextricably linked to us and the activity that we carry out on Web3. These domain NFTs have the potential to represent a house in the Metaverse, thereby registering and validating all guests, maintenances, and occasions. And that record and that infrastructure can be sold along with the house, or even as vital component of it, thereby boosting the worth of the property.

3.2.1.3 Comparing the Metaverse and NFTs: Foundations, Origins, and Usability

Many of you probably saw the internet as we know it today as an idealized version of the previous version. However, beneath the surface of web 2.0, or the internet as we know and use it today, there are a great deal of complexities. For instance, the fact that centralized companies have control over the data of users is a major blow to the protection of user privacy.

The ideas of the Metaverse and non-fungible tokens (NFTs) are completely changing the trajectory of the internet's development. The primary distinction between NFT and the Metaverse can be traced back to the fundamental meanings of both terms. To put it simply, non-fungible tokens are a specific kind of virtual token, and the Metaverse is its very own independent virtual world.

Foundations: The definition of NFTs as well as the Metaverse offer sufficient grounds for conducting an efficient comparison between the two. You should take note of the fact that the use of Blockchain technology serves as the fundamental basis for the comparison between NFT and the Metaverse. This is an important point. Because it is essential for the development of smart-contracts, which dictate who owns the NFTs and the transactions that can be conducted with them, Blockchain is an essential component of non-fungible tokens (NFTs).

The Metaverse, on the other hand, is a large world that is based on the vision of creating an internet that is open, shared, persistent, and highly interactive. Immutability, the inability to be exchanged for other currencies, and security are the distinguishing characteristics of non-fungible tokens. On the other hand, the Metaverse gives users access to a wide variety of characteristics, such as decentralization, user identity, the economy of creators, and experiences.

Origins: The first implementation of NFTs occurred in 2017 with the launch of CryptoPunks, which dates back many years. During this time period, the CryptoKitties collection was also mentioned in the media for contributing to congestion on the Ethereum network. The history of non-fungible tokens (NFTs) hints at the possibility of developing new assets on the Blockchain that can denote individual ownership. Because of this, the introduction of NFTs may have unintentionally led to new developments that make it easier for people to own assets in different places.

The comparison of the NFT and the Metaverse in terms of their origins sheds light on the aspirations and objectives that lie behind each technology. When it comes to goals, the Metaverse lacks even a single overarching objective. It makes decentralization better and makes it possible to apply it in a variety of other contexts. The concept of the Metaverse first appeared in a science fiction book, in which it was described as a place where one could go to get away from the "real world."

Usability: The usability of a non-fungible token is going to be the next significant facet to be highlighted when comparing it to a Metaverse. How straightforward is it for you to get onto the NFTs or the Metaverse platforms? You can get your hands on the best

NFTs by using one of the many platforms that are available, such as a marketplace for NFTs. OpenSea is currently the largest marketplace for non-fungible tokens (NFTs). Before buying non-fungible tokens (NFTs), users can look around OpenSea to learn all about the features of the tokens.

You would also find out that the Metaverse can be easily accessed through a variety of different platforms. Users have access to a variety of Metaverse platforms, including the Sandbox Metaverse, the Roblox gaming Metaverse, and other platforms, most notably the Facebook meta platform. To enter any Metaverse platform, all you need is a collection of your preferred virtual reality (VR) or extended reality (XR) devices.

3.2.2 Ether Legends

Ether Legends is an artful, lighthearted NFT Blockchain collectible trading card game that’s powered by Enjin, Polygon and the Ethereum Network. Players have the opportunity to earn via playing and while collecting NFT companions and characters in order to engage in the multi-player trading card game more intensively.

Ether Legends is a unique concept that’s based on collecting various tokens for in-game modifiers to earn more, with engaging PVP battle that offers players to continually scale up their characters, companions and more.

The first-of-its-kind game platform that makes it easy for trading cards to be redeemed digitally, seen, played, traded, or sold as digital assets and gives the whole world a place to buy and sell them.

Ether Legends, a game built on the Ethereum Blockchain, is the first game to come out on this platform. It’s beautiful illustrations, design, and skill-based game play set it apart as a true original and leave room for the platform to grow and for more games to come out. The Elementeum token is both a reward and a currency on this gaming platform. It helps the digital ecosystem work.

ETHER LEGENDS
MEN & BEASTS
WWW.ETHERLEGENDS.COM
COMMON
RARE
EPIC
LEGENDARY

Figures 10. Ether Legends Trading Cards of NFTs

Sources: (Nayl, 2022)

According to recent research by individuals and governments, the Blockchain and NFT space is one of the most rapidly and significantly expanding, with people investing more time and money. It is forecasted that worldwide expenditure on Blockchain-based solutions will reach approximately $6.6 billion by the end of 2021, with a projected increase to $19 billion by the end of 2024, according to Statista. The integration of Blockchain technologies is expected to drive growth in the gaming industry, particularly in the realm of owning and tokenizing game content.

Elementeum Games is a devoted sponsor of Blockchain-based games that is well-known for promoting current trends that demonstrate the potential for exponential growth. This is why they wanted to provide a platform for people to use Blockchain technology to earn money, own digital assets (via non-fungible tokens, or NFTs), and have fun in an interactive, gamified environment.

TekRevol has successfully completed and released a player-focused game with a seamless integration of Blockchain fundamentals and continues to work on scaling aspects, single player (AI), and other concepts that had to be put on hold in order to stabilize the game. Future concepts include additional Blockchain integration, game mechanics, and the capacity for players to claim NFTs through the app interfaces.

The Ether Legends game is interactive and easy to use. It has interesting characters, artwork, and environments that make the game more fun, as well as player-owned assets and a system that lets you play to earn.

Elementeum Gaming, LLC's goal is to be the go-to service for online trading card games. We want to provide the best possible environment for players to earn, buy, sell, and trade online while maintaining full control over their digital possessions. The team's goal is to make a collectible card game where players feel a deep connection to the Ether Legends characters, engage in challenging yet fair match play, gain rewards for their efforts, and have a great time doing so.

4. CONCLUSION

In this paper, we examined the underlying technologies that enable non-fungible tokens (NFTs) and explored the various security challenges that these tokens face. By analyzing key concepts such as Blockchain technology, smart contracts, and online marketplaces, we were able to provide a comprehensive overview of the NFT landscape. We then delved into specific challenges facing NFTs, including issues related to privacy, security, and scalability, and evaluated potential solutions or mitigations to these challenges. Overall, our analysis highlights the need for ongoing research and development in the NFT space in order to address the security challenges that these tokens pose.

Non-fungible tokens (NFTs) are a relatively new and rapidly evolving technology, and it is clear that significant changes are on the horizon as they continue to mature. Despite their immaturity and inherent instability, NFTs have gained tremendous popularity in a short period of time, and it seems certain that they will continue to be a major force in the digital world. As we have seen, NFTs have the potential to transform various aspects of our daily lives, including the way we use services, the transparency of transactions, and the way we think about ownership of real estate, artwork, ideas, and concepts. It is likely that the NFT space will continue to evolve and advance at a rapid pace in the coming years, and we can expect to see significant disruptions and innovations in this field.

REFERENCES

Articles

Ali, O., Momin, M., Shrestha, A., Das, R., Alhajj, F., & Dwivedi, Y. K. (2022). A review of the key challenges of non-fungible tokens. *Technological Forecasting and Social Change*, *187*, 122248.

Ambrasaitė P. and Smagurauskaitė A. (2021) “Epic Games v. Apple: Fortnite battle that can change the industry”, Vilnius University Open Series, pp. 6-25. doi: 10.15388/TMP.2021.1.

Aristidou, A., Shamir, A., & Chrysanthou, Y. (2019). Digital dance ethnography: Organizing large dance collections. *Journal on Computing and Cultural Heritage (JOCCH)*, *12*(4), 1-27.

Babel, M., Gramlich, V., Körner, M. F., Sedlmeir, J., Strüker, J., & Zwede, T. (2022). Enabling end-to-end digital carbon emission tracing with shielded NFTs. *Energy Informatics*, *5*(1), 1-21.

Bernstein. (2021). 5 business use cases for NFTs | TechTarget. WhatIs.com. Retrieved July 17, 2021, from https://www.techtarget.com/whatis/feature/5-business-use-cases-for-NFTs

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

Boireau, O. (2018). Securing the Blockchain against hackers. *Network Security*, *2018*(1), 8-11.

Chohan, R., & Paschen, J. (2021). What Marketers Need to Know about Non Fungible Tokens (NFTs). Business Horizons.

Ciaian, P., Rajcaniova, M., & Kancs, D. (2016). The Economics of BitCoin Price Formation. Applied Economics, 48(19), 1799–1815

Colavizza, G., Finucane, B., Franceschet, M., Hernández, S., Morgan, J., Ostachowski, M. L., ... & Scalet, S. (2020). T’ai Smith.«Crypto Art: A decentralized view». *Leonardo*, 1-8.

Dionisio, J. D. N., III, W. G. B., & Gilbert, R. (2013). 3D virtual worlds and the Metaverse: Current status and future possibilities. *ACM Computing Surveys (CSUR)*, *45*(3), 1-38.

Durham, J. (1965). Confusion of Fungible and Non-Fungible Goods. Baylor Literature Review, 17, 80–89

Dwyer, G. P. (2015). The Economics of Bitcoin and Similar Private Digital Currencies. Journal of Financial Stability, 17(2015), 81–91.

Evans, T. M. (2019). Cryptokitties, Cryptography, and Copyright. AIPLA QJ, 47, 219.

Fairfield, J. (2021). Tokenized: The law of non-fungible tokens and unique digital property. *Indiana Law Journal, Forthcoming*.

Focus. (2021). The First NFT Millionaire Made It Possible for Anyone to Earn $171,000 A Month by Investing. Retrieved January 18, 2022, from https://focus.com.au/first-nft- project-on- opensea

Forbes. (2021). NFTs, Metaverse and GameFi Are Changing Up the Fashion Business in 2022. Retrieved February 2, 2022, from https://www.forbes.com/sites/josephdeacetis/2021/12/22/nfts-Metaverse-and-gamefi- are-changing-up-the-fashion-business-in-2022

Gorkhali, A., Li, L., & Shrestha, A. (2020). Blockchain: A Literature Review. Journal of Management Analytics, 7(3), 321–343.

Gupta, S. S. (2017). Blockchain: IBM Online. Retrieved December 23, 2021, from http://www.ibm.com

Holds, M. (2019). *What is a Re-Entrancy Attack?* What Is a Re-Entrancy Attack? Retrieved December 11, 2022, from https://quantstamp.com/blog/what-is-a-re-entrancy-attack

Hoory, L. (2022). *Are Secret NFTs a Solution to NFT Privacy Problems*? Retrieved December 14, 2022, from https://blockpit.io/unchained/en/secret-nfts/

Joshua. (2017). Information bodies: Computational anxiety in Neal Stephenson's snow crash. Interdiscipl. Literary Stud., 19(1), 17-47. Retrieved from https://www.jstor.org/stable/10.5325/intelitestud.19.1.0017

Kain E., “Epic games pulls Travis Scott emote from ‘fortnite’ item shop,” Accessed: Dec. 16, 2021. [Online]. Available: https://www.forbes.com/sites/erikkain/2021/11/09/epic-gamespulls-travis-scott-emote-from-fortnite-item-shop/?sh=7f5cbabe4708

Kamenov, K. (2017). Immersive Experience—The 4th Wave in Tech: Learning the Ropes.

Kinyua. (2022). *Security Threats for NFTS and Possible Solutions*. Engineering Education (EngEd) Program | Section. Retrieved December 17, 2022, from https://www.section.io/engineering-education/security-threats-of-nfts-and-possible-solutions-hardware-wallet/

LaDuke, W. (1994). Traditional ecological knowledge and environmental features. Colo. J. Int'l Envtl. L. & Pol'y, 5, 127

Lambert, N. (2021). Beyond nfts: A possible future for digital art. *ITNOW, 63*(3), 8-10.

Lin, I. C., & Liao, T. C. (2017). A survey of Blockchain security issues and challenges. *Int. J. Netw. Secur., 19*(5), 653-659.

Lu, Q., Xu, X., Bandara, H. D., Chen, S., & Zhu, L. (2021). Patterns for Blockchain-based payment applications. In *26th European Conference on Pattern Languages of Programs* (pp. 1-17).

Mahdad. Kiyani. (2021). Let's talk NFT and Digital Ownership! Retrieved from: https://www.linkedin.com/pulse/lets talk nft digital ownership mahdad kiyani/

Maxmudjanovna, A. I., Abdurasulovna, P. R., & Erkinovna, N. N. (2020). The Future of the Digital Economy: Concept and Role of Blockchain Technologies. Journal of Critical Reviews, 7(8), 1812–1818.

Meta, “Introducing Meta: A social technology company,” Accessed: Dec. 16, 2021. [Online]. Available: https://about.fb.com/news/2021/10/facebook-company-is-now-meta/

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

Nadini, M., Alessandretti, L., Di Giacinto, F., Martino, M., Aiello, L. M., & Baronchelli, A. (2021). Mapping the NFT Revolution: Market Trends, Trade Networks, and Visual Features. Scientific Reports, 11(1), 1–11.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from Bitcoin.

Nayl. (2022, March). Ether Legends Item Shop. Ether Legends Item Shop. Retrieved March 2022, from https://www.etherlegends.com/store/men-and-beasts.html

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. Business & Information. Systems Engineering, 59(3), 183–187.

O’Dwyer, R. (2020). Limited Edition: Producing Artificial Scarcity for Digital Art on the Blockchain and Its Implications for the Cultural Industries. Convergence, 26(4), 874–894.

Park, S., Specter, M., Narula, N., & Rivest, R. L. (2021). Going from Bad to Worse: From Internet Voting to Blockchain Voting. Journal of Cybersecurity, 7(1), 25–31.

Patel, N. (2022, September 10). NFT Metadata Example, Standards and Format | NFT JSON Metadata. Makeanapplik. Retrieved December 24, 2022, from https://makeanapplike.com/nft-metadata-example-and-standards/

Pratap, Z. (2022). *Reentrancy Attacks and The DAO Hack Explained | Chainlink*. Chainlink Blog. Retrieved December 11, 2022, from https://blog.chain.link/reentrancy-attacks-and-the-dao-hack/

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain Technology and Its Relationships to Sustainable Supply Chain Management. International Journal of Production Research, 57(7), 2117–2135

SCRT Labs. (2022). Secret NFTs. Retrieved November 24, 2022, from https://scrt.network/about/secret-nfts

Seok, B., Park, J., & Park, J. H. (2019). A Lightweight Hash-Based Blockchain Architecture for Industrial IoT. Applied Sciences, 9(18), 3740–3745.

Serada, A., Sihvonen, T., & Harviainen, J. T. (2021). CryptoKitties and the New Ludic Economy: How Blockchain Introduces Value, Ownership, and Scarcity in Digital Gaming. Games and Culture, 16(4), 457–480.

Shah, D., Patel, D., Adesara, J., Hingu, P., & Shah, M. (2021). Exploiting the Capabilities of Blockchain and Machine Learning in Education. Augmented Human Research, 6(1), 1–14.

Sillaber, C., & Waltl, B. (2017). Life cycle of smart contracts in Blockchain ecosystems. *Datenschutz und Datensicherheit-DuD*, *41*(8), 497-500.

Singh, J., & Singh, P. (2021). Distributed Ownership Model for Non-Fungible Tokens. Smart and Sustainable Intelligent Systems, 12, 307–321.

Song, J. Y., Chang, W., & Song, J. W. (2019). Cluster Analysis on the Structure of the Cryptocurrency Market via Bitcoin-Ethereum Filtering. Physica A: Statistical Mechanics and Its Applications, 527, 121339–121345.

Sparango, B. (2018). “The Rise of Non-Fungible Token Assets.” Retrieved from https://medium.com/coinmonks/the-rise-of-non-fungible-token-assets-7fdb4bbb8ad7

Swami, R., Dave, M., & Ranga, V. (2019). Software-defined Networking-based DDoS Defense Mechanisms. ACM Computing Surveys, 52(2), 1–36. https://doi.org/10.1145/3301614

Sylim, P., Liu, F., Marcelo, A., & Fontelo, P. (2018). Blockchain Technology for Detecting Falsified and Substandard Drugs in Distribution: Pharmaceutical Supply Chain Intervention. JMIR Research Protocols, 7(9), e10163–e10172.

Szabo, N. (1996). Smart contracts: Building blocks for digital markets. Retrieved from https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Tech, “Beamlink,” Accessed: May 16, 2022. [Online]. Available: https://www.jingtengtech.com/home/mr-meeting.html

Themistocleous, M. (2018). Blockchain Technology and Land Registry. Cyprus Review, 30(2), 195–202.

Uribe, D., & Waters, G. (2020). Privacy laws, genomic data and non-fungible tokens. *The Journal of the British Blockchain Association*, 13164.

Usmani, S. S., Sharath, M., & Mehendale, M. (2022). Future of mental health in the Metaverse. *General Psychiatry*, *35*(4), e100825.

Vashchuk, O., & Shuwar, R. (2018). Pros and cons of consensus algorithm proof of stake. Difference in the network safety in proof of work and proof of stake. Electronics and Information Technologies, 9. https://doi.org/10.30970/eli.9.106

Wang, Q., Qin, B., Hu, J., & Xiao, F. (2020). Preserving transaction privacy in bitcoin. *Future Generation Computer Systems*, *107*, 793-804.

Weston G. NFTs and their role in the “Metaverse”. Available: https://101Blockchains.com/nfts-and-Metaverse/ [Accessed 08 Feb 2022].

Whitaker, A., Bracegirdle, A., de Menil, S., Gitlitz, M. A., & Saltos, L. (2021). Art, Antiquities, and Blockchain: New Approaches to the Restitution of Cultural Heritage. International Journal of Cultural Policy, 27(3), 312–329.

White, B., Mahanti, A., & Passi, K. (2022). Characterizing the OpenSea NFT Marketplace. In *Companion Proceedings of the Web Conference 2022* (pp. 488-496).

Wilson, K. B., Karg, A., & Ghaderi, H. (2021). Prospecting Non-Fungible Tokens in the Digital Economy: Stakeholders and Ecosystem, Risk and Opportunity. Business Horizons.

Wired. (2021). NFT e Musica. Perché Sono Fatti l'Uno per l'Altro? Retrieved October 31, 2021, from https://www.wired.it/play/musica/2021/07/03/nft-musica-funzionano/

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

Zhai, S., Yang, Y., Li, J., Qiu, C., & Zhao, J. (2019). Research on the Application of Cryptography on the Blockchain. Journal of Physics: Conference Series, 1168(3), 032077–032089.

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International journal of web and grid services, 14(4), 352-375.

Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X., Weng, J., Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. Future Generation Computer Systems, 105, 475-491. https://doi.org/10.1016/j.future.2019.12.019

Zhou, J., & Gollman, D. (1996). A fair non-repudiation protocol. In *Proceedings 1996 IEEE Symposium on Security and Privacy* (pp. 55-61). IEEE.

Books

Atzei, N., Bartoletti, M., and Cimoli, T. A survey of attacks on Ethereum smart contracts (sok). In Principles of Security and Trust (2017), M. Maffei and M. Ryan, Eds., Springer Berlin Heidelberg, pp. 164–186.

Jeon, H. J., Youn, H. C., Ko, S. M., & Kim, T. H. (2022). Blockchain and AI Meet in the Metaverse. *Advances in the Convergence of Blockchain and Artificial Intelligence*, *73*.

Li, R., Galindo, D., & Wang, Q. (2019). Auditable credential anonymity revocation based on privacy-preserving smart contracts. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology* (pp. 355-371). Springer, Cham

Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). *Handbook of applied cryptography*. CRC press.

Pilkington, M. (2016). Blockchain Technology: Principles and Applications. In F. X. Olleros & M. Zhegu (Eds.), Research Handbook on Digital Transformations (pp. 41–48). Edward Elgar Publishing.

Sestino, A., Giraldi, L., Cedrola, E., & Guido, G. (2022). The Relevance of Individuals' Perceived Data Protection Level on Intention to Use Blockchain-Based Mobile Apps. An Experimental Study. In M. Al-Emran (Ed.), Recent Innovations in Artificial Intelligence and Smart Applications. Springer International Publishing, in press.

Singhal, B., Dhameja, G., & Panda, P. S. (2018). How Blockchain Works. In B. Singhal, G. Dhameja, & P. S. Panda (Eds.), Beginning Blockchain (pp. 31–148). Apress.

Sestino, A., Guido, G., & Peluso, A. M. (2022). Non-Fungible Tokens (NFTs): Examining the Impact on Consumers and Marketing Strategies. Retrieved from doi:10.1007/978-3-031-07203-1.

Papers

Ante, L. The non-fungible token (NFT) market and its relationship with Bitcoin and Ethereum (2021). *Available at SSRN: https://ssrn.com/abstract, 3861106*.

Beck, R., J. Stenum Czepluch, N. Lollike and S. Malone. (2016). "Blockchain – The Gateway to Trust-Free Cryptographic Transactions." In: *Twenty-Fourth European Conference on Information Systems (ECIS), İstanbul,Turkey, 2016.* (pp. 1–14). Springer Publishing Company.

Buterin, V. (2014). "A next-generation smart contract and decentralized application platform." changing-up- the- fashion- business- in- 2022

Capital G., "Metaverse property," Accessed: Nov. 11, 2021. [Online]. Available: https://Metaverse.properties/buy-in-decentraland/

Das, D., Bose, P., Ruaro, N., Kruegel, C., & Vigna, G. (2021). Understanding security Issues in the NFT Ecosystem. *arXiv preprint arXiv:2111.08893*.

Delmolino, K., Arnett, M., Kosba, A., Miller, A., & Shi, E. (2016). Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. In International conference on financial cryptography and data security (pp. 79-94). Springer, Berlin, Heidelberg.

Digiconomist. (2021). Ethereum Energy Consumption Index (beta) - Digiconomist. https://digiconomist.net/ethereum-energy-consumption

El Faqir, El Rhazoui, Y. (2021). Decentralized Autonomous Organizations on Blockchain: Analysis and visualization.

Epic Games, "Fortnite," Epic Games, 2017.

Epic Games, "The world's most open and advanced real-time 3D creation tool," Accessed: Dec. 16, 2021. [Online]. Available: https://www.unrealengine.com/en-US/

Ferguson, S., Schubert, E., & Stevens, C. J. (2014). Dynamic dance warping: Using dynamic time warping to compare dance movement performed under different conditions. In *Proceedings of the 2014 international workshop on movement and computing* (pp. 94-99).

Glaser, F. (2017). Pervasive decentralisation of digital infrastructures: a framework for Blockchain enabled system and use case analysis.

Horizen. (2022). Academy, *Attacks on Blockchain,* Retrieved December 11, 2022, from https://www.horizen.io/Blockchain-academy/technology/advanced/attacks-on-Blockchain/

Houben, R., & Snyers, A. (2018). *Cryptocurrencies and Blockchain: Legal context and implications for financial crime, money laundering and tax evasion*.

Jacques, D., Jordi, B., & Thomas, S. (2017). EIP-777: ERC-777 token standard. Retrieved from https://eips.ethereum.org/EIPS/eip-777

Jimi, S. (2018). Blockchain explained: how a 51% attack works double spend attack.

Jørgensen, K. P., & Beck, R. (2022). Universal Wallets. *Business & Information Systems Engineering*, *64*(1), 115-125.

Kasireddy, P. (2017). How does Ethereum work, anyway. *Medium*.

Krupa, T., Ries, M., Kotuliak, I., & Bencel, R. (2021). Security issues of smart contracts in ethereum platforms. In *2021 28th Conference of Open Innovations Association (FRUCT)* (pp. 208-214). IEEE.

Lee, L. H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., ... & Hui, P. (2021). All one needs to know about Metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. *arXiv preprint arXiv:2110.05352*.

Liu, F., Li, R., Wang, Q., Wang, Q., & Galindo, D. (2020). An accountable decryption system based on privacy-preserving smart contracts. In *International Conference on Information Security* (pp. 372-390). Springer, Cham.

Milgram, P., Takemura, H., Utsumi, A., & Kishino, F. (1995). Augmented reality: A class of displays on the reality-virtuality continuum. In *Telemanipulator and telepresence technologies* (Vol. 2351, pp. 282-292). Spie.

Moubarak, J., Filiol, E., & Chamoun, M. (2018). On Blockchain security and relevant attacks. In *2018 IEEE Middle East and North Africa Communications Conference (MENACOMM)* (pp. 1-6). IEEE.

Musamih, A., Salah, K., Jayaraman, R., Yaqoob, I., Puthal, D., & Ellahham, S. (2022). NFTs in healthcare: Vision, opportunities, and challenges. *IEEE Consumer Electronics Magazine*.

Musienko, Y. (2022). *How to Make NFTs Secure? - Merehead*. Merehead. Retrieved December 11, 2022, from https://merehead.com/blog/make-nfts-secure/

Noether, S. (2015). Ring signature confidential transactions for monero. IACR Cryptol.

Oliveira, L., Zavolokina, L., Bauer, I., & Schwabe, G. (2018). To Token or Not to Token: Tools for Understanding Blockchain Tokens. Retrieved December 28, 2021, from https://www.zora.uzh.ch/id/eprint/157908/

Parham, A., & Breitinger, C. (2022). Non-fungible Tokens: Promise or Peril? *arXiv preprint arXiv:2202.06354*.

Raman, R. K., Vaculin, R., Hind, M., Remy, S. L., Pissadaki, E. K., Bore, N. K., ... & Varshney, K. R. (2018). Trusted multi-party computation and verifiable simulations: A scalable Blockchain approach. *arXiv preprint arXiv:1809.08438*.

Regner, F., Urbach, N., & Schweizer, A. (2019). NFTs in practice–non-fungible tokens as core component of a Blockchain-based event ticketing application.

Rezaeighaleh, H., & Zou, C. C. (2019). New secure approach to backup cryptocurrency wallets. In *2019 IEEE Global Communications Conference (GLOBECOM)* (pp. 1-6). IEEE.

Rodrigues, B., Bocek, T., Lareida, A., Hausheer, D., Rafati, S., & Stiller, B. (2017, July). A Blockchain-based architecture for collaborative DDoS mitigation with smart contracts. In *IFIP International Conference on Autonomous Infrastructure, Management and Security* (pp. 16-29). Springer, Cham.

Schweizer, A., V. Schlatt, N. Urbach and G. Fridgen. (2017). “Unchaining Social Businesses - Blockchain as the Basic Technology of a Crowdlending Platform.” In: *38th ICIS*.

Seymour M., C. Evans, and K. Libreri, “Meet mike: Epic avatars,” in Proc. ACM SIGGRAPH VR Village, 2017, pp. 1–2.

Shirole, M., Darisi, M., & Bhirud, S. (2020). Cryptocurrency token: an overview. *IC-BCT 2019*, 133-140.

Swathi, P., Modi, C., & Patel, D. (2019). Preventing Sybil Attack in Blockchain using Distributed Behavior Monitoring of Miners. In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT). doi:10.1109/icccnt45670.2019.8944507

Wang, Q., Li, R., Wang, Q., & Chen, S. (2021). Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges. Retrieved December 1, 2021, from https://arxiv.org/abs/2105.07447

William, E., Dieter, S., Jacob, E., & Nastassia, S. (2018). Erc-721 non-fungible token standard. Ethereum Improvement Protocol, EIP-721. *Ethereum*.

Witek, R., Andrew, C., Philippe, C., James, T., Eric, B., & Ronan, S. (2018). Eip-1155: Erc-1155 multi token standard. Ethereum Improvement Protocol, EIP-1155.

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

Zhu, Chris, "NFT Sneaker Marketplace Design, Testing, and Challenges" (2022). Honors Theses. Paper 1385. https://digitalcommons.colby.edu/honorstheses/1385

Zohar, A. (2015). Bitcoin: under the hood. *Communications of the ACM*, *58*(9), 104-113.