CORSO DI LAUREA IN: XXXXXXX X XXXXXXXXXX XXXXXXXXXX

NFTS IN THE DIGITAL AGE: CYBERSECURITY RISKS AND AI-POWERED SMART CONTRACT SOLUTION

TIPO TESI: (sperimentale, compilativa, di ricerca)

Studente:
GIACOMO BERTAZZOLO

Relatore:
VALENTINA GATTESCHI

ANNO ACCADEMICO 2022-2023

dedica.

Table of Contents

Abstract

The burgeoning realm of blockchain technology, underpinning the foundation of modern cryptographic systems, serves as a focal point for this master's thesis. Central to this exploration is the emergence of Non-Fungible Tokens (NFTs), cryptographic assets unique in their representation and utility. This research commences with an elucidation of blockchain's theoretical underpinnings, followed by a chronological delineation of NFTs, emphasizing their evolutionary trajectory and inherent value propositions within a cryptographic context.

Subsequently, the study undertakes a rigorous quantitative and qualitative analysis of the current NFT market. Methodical segmentation reveals nuanced market vectors, each delineated and assessed based on its unique characteristics. Analytical scrutiny of predominant marketplaces and platforms is also presented, emphasizing their operational paradigms and influence on NFT liquidity and valuation. Drawing on empirical data, recent market trends are critically evaluated, providing a comprehensive understanding of the market's dynamic equilibrium.

Pivoting to the domain of cybersecurity, the research meticulously categorizes a spectrum of risks that permeate the NFT infrastructure. Employing a taxonomy of cyber threats, the work highlights potential vulnerabilities, delineates attack vectors, and characterizes the modus operandi of potential scams targeting the NFT ecosystem.

In response to the identified threats, the thesis introduces a novel security paradigm: an integration of blockchain's deterministic consensus algorithms with advanced artificial intelligence tools. The capabilities of a specific tool, sourced from the start-up Anchain.AI, are critically assessed, underscoring its potential for real-time threat detection and mitigation within the NFT domain.

The research culminates with a robust evaluation of this integrated solution, employing both computational benchmarks and theoretical analysis to determine its efficacy, scalability, and potential implications. The objective remains to underscore the importance of robust security

protocols and to elucidate a path forward for the sustainable growth of the NFT market, ensuring its resilience in the face of evolving cyber threats.

1. Introduction

As the NFT sector continues to evolve and mature, the importance of robust security cannot be understated. The recent downturn in the NFT and cryptocurrency market in 2022 highlighted not only economic challenges but also the inherent vulnerabilities within the ecosystem. The increasing prevalence and sophistication of attacks make this research not just relevant, but vital.

In an environment where transactions are irreversible, and the decentralized nature means there's no central entity for oversight or control, attacks can have devastating consequences. These threats not only jeopardize economic value but also erode trust in the system, a crucial element for its broad-scale adoption. The challenge in detecting such attacks, given the absence of traditional oversight mechanisms, further exacerbates the situation.

The need for innovative and effective security solutions is palpable. This research, exploring both the nature of the attacks and potential solutions, seeks to bridge this gap, proposing strategies and mechanisms to safeguard users and maintain the integrity of the NFT world.

In light of the emerging challenges in the NFT ecosystem, this study aims to address and answer several pressing questions:

NFT Marketplaces' Vulnerabilities: What are the inherent vulnerabilities of NFT marketplaces, and how can these be exploited by malicious actors? Exploring and pinpointing these gaps is crucial for understanding the threat landscape and crafting effective solutions.

Fraudulent Activities by Malicious Users: Are malicious actors directly involved in fraudulent activities leading to financial losses for everyday users? Identifying and analyzing such fraudulent schemes can offer insights into the nature and extent of the threat.

User Protection: What strategies and solutions can be implemented to prevent financial losses and ensure user safety within the NFT ecosystem? Proposing efficient and effective solutions is key to restoring and maintaining trust in the technology.

To ensure the robustness and comprehensiveness of this research, a two-phase methodology was adopted. The initial phase of the research, Documentary Analysis, delved deeply into the examination of existing research papers and studies pertinent to the NFT topic. Such a review of literature laid down a firm theoretical foundation, bringing to light the current trends, emerging challenges, and solutions previously proposed in the realm of NFTs and their security. Following this, in the subsequent phase, an Evaluation of the Proposed Solution was carried out. Upon detailing and formulating the solution powered by an AI-enhanced smart contract, a rigorous assessment took place. This assessment pivoted around two main criteria: the amplified transaction cost and the duration of the transaction. It is paramount to understand these elements, ensuring that the solution, while bolstering security, also operates efficiently and remains economically feasible for users.

This research has been structured to offer a comprehensive overview of the NFT domain, from its foundations to emerging challenges, to innovative solutions proposed. The detailed structure of the thesis is as follows:

State-of-the-art Analysis: This section is dedicated to providing a thorough overview of the NFT ecosystem, exploring its origins, evolution, major trends, and key players.

Cyber Risk in the NFT Ecosystem: This part shifts focus to risks associated with NFTs in terms of cybersecurity, examining major attack vectors, known vulnerabilities, and significant incidents in the sector.

Proposed Solution: Building on the challenges and vulnerabilities identified in previous sections, this part introduces an innovative solution. The solution, leveraging an AI-powered smart contract, aims to provide a defence mechanism against malicious actors in the NFT world.

Performance Evaluation: The thesis's final segment is dedicated to the practical evaluation of the proposed solution. Key criteria such as the increased transaction cost and transaction time will be considered, ensuring the solution is effective and feasible for users.

With the rise of NFTs and their increasing significance across various sectors, it's imperative to address the security challenges accompanying this digital revolution. As NFTs represent a notable leap towards digital ownership and decentralization, they bring along a new set of vulnerabilities requiring profound understanding and ingenious solutions. Through state-of-the-art analysis, risk exploration, and the proposal of smart contract and AI-based solutions, this thesis aims to light the path towards a safer, more resilient NFT ecosystem. Ultimately, the goal is to ensure the promise of NFTs is not overshadowed by the spectres of security risks but is rather enhanced by strong protective measures and awareness.

1.1. **General info**

Blockchain technology can disrupt or replace existing business models relying on third parties for trust. The blockchain concept was first introduced in 2008 through the release of the Bitcoin whitepaper (Nakamoto, 2008) and was initially used primarily for cryptocurrencies.

In 2014, a second generation of blockchains (e.g., Ethereum) was introduced, which allows for the creation and execution of Smart Contracts on all participating Blockchain nodes. This has opened the possibility of using blockchain in various industries, including supply chain management, international payments, international trade finance, energy markets, and notary services. Remarkably, the use cases of Initial Coin Offerings (ICOs) that reinvent crowdfunding through blockchain and its ability to tokenize assets are drawing public attention.

In contrast, non-fungible tokens (NFTs), unlike traditional cryptocurrencies, which are interchangeable and easily replicated, are unique and cannot be replicated or replaced. This characteristic makes them valuable for representing ownership of digital items and has led to the growth of a thriving market. This thesis will explore the state of the art of NFTs and their potential implications and threats. We will also examine the challenges and opportunities the growing NFT market presents and discuss the cybersecurity issue.

1.2. History

The concept of NFTs can be traced back to the early days of blockchain technology, which first emerged in 2009 with the launch of the Bitcoin network. However, it was only with the emergence of Ethereum in 2015 that the idea of NFTs began to take shape.

Ethereum is a blockchain platform allowing users to create and execute smart contracts, self-executing agreements with terms written into code. This enabled developers to create unique digital tokens that could not be replicated or replaced, a key feature of NFTs.

The widespread adoption of NFTs will likely significantly impact various industries as they enable new forms of ownership and monetization. In order to understand how the NFT space might develop, it is helpful to consider the history of NFTs, which began with Colored Coins. Colored Coins, considered the predecessors of modern NFTs, are not the same as NFTs as we currently understand them. Rather than being tokens with complex infrastructure that can support various digital assets, Colored Coins are simply Bitcoins or small units of Bitcoin.

(Satoshi) that have been marked with unique ID information. This allows every Bitcoin to be identified and its history tracked. These markings can be used to determine their purpose, such as representing realworld assets on the blockchain. However, they do not have the capabilities of today's NFTs.

On December 4th, 2012, Meni Rosenfeld, a cryptographer and the President of the Israeli Bitcoin Association, published a paper titled "Overview of Colored Coins." In this paper, Rosenfeld explained a mechanism for using Bitcoin's "fungibility" to segregate certain coins for particular purposes, allowing the creation of niche applications within the Bitcoin blockchain. He suggested that this could be done by adding "specialty" to coins by segregating them from the rest.

In closed or permissioned environments, users added extra data to transactions, such as messages or other custom information (for example, third-party application IDs and hashed documents in Merkle Trees). This allowed tokens to be customized with metadata, which could be used to represent a real-world asset that had been digitized and layered on top of Bitcoins on the blockchain. As a result, these custom coins could be used to track and verify ownership of physical assets.

Colored Coins were initially intended to replace many costly and time-consuming financial transactions. For example, property deeds could be appended to a colored coin, and the transfer of the coin itself could be used to represent property ownership or, in other cases, to track the ownership of commodities and bonds. However, the limitations of Colored Coins soon became apparent. The value attributed to them required unanimous consensus from participants and the issuer to redeem them for the real-world asset unconditionally. If a participant refused to accept a coin in exchange for a physical asset, there was no way to enforce the transaction. In addition, if the system were only being used to track asset transfers, a simple permissioned database would be more efficient than using the secure but inefficient infrastructure of the Bitcoin blockchain.

While Colored Coins played a significant role in demonstrating the potential of digital non-fungible assets on the blockchain, better solutions soon emerged. More expressive protocols allowed for complex and sophisticated implementations of non-fungibility, and public interest quickly shifted toward these networks. For example, in 2014, the peer-to-peer financial platform Counterparty was created on top of the Bitcoin blockchain. It featured a variety of tools, including wallets, escrow functionality, a central clearing counterparty, a decentralized exchange, and a native currency called XCP. Counterparty became a hub for many projects and non-fungible assets, including a trading card game. At the same time, work was also underway on the Ethereum ecosystem. Three months after the launch of Ethereum's main net, the Etheria project introduced a virtual open world composed of hexagonal tiles that could be bought, sold, and built upon as NFTs. Counterparty and Ethereum showed that NFTs were evolving beyond their primitive origins with Colored Coins.

The year 2017 marked a milestone for NFTs. The first actual project based on the scarcity of digital assets entirely native to the Ethereum network was launched. Ten thousand tokens were launched, each with different characteristics whose combination defined the total scarcity. The initiative, dubbed Cryptopunks in honour of the original cypherpunks behind Bitcoin, provided the groundwork for what we now know as NFTs.

The initiative was dubbed Cryptopunks, echoing the initial period of Bitcoin's cypherpunks, and laid the groundwork for the modern understanding of NFTs. After the rise of Cryptopunks, various other NFT projects came into existence. However, this sphere gained widespread recognition only with the advent of the ERC721 token standard on the Ethereum blockchain, marking the introduction of the term NFT.

The already cited ERC-721, a standard designed explicitly for NFTs, was introduced in the same year. The inaugural project leveraging this standard was CryptoKitties, a game rooted in blockchain technology that allowed players to virtually adopt, nurture, breed, and trade cartoon-like felines. This initiative was brought to life by Axiom Zen, a Vancouver-based company, and gained significant attention during the ETH Waterloo Hackathon.

CryptoKitties had a profound impact on the NFT landscape for three key reasons:

1. They served as one of the earliest examples of blockchain's potential application in the gaming industry, thereby gaining the recognition and validation of many observers.
2. The project demonstrated the need for adaptable and expressive protocols like Ethereum. Their "raising" and "breeding" features were an early model for the comprehensive interoperability found in current DeFi applications.
3. Moreover, CryptoKitties drew attention to the constraints of blockchain and led to the wide dissemination of the concept known as the blockchain trilemma.

The game's immense popularity and the high volume of transactions it generated occasionally rendered the Ethereum blockchain inoperable. Recent advancements in NFTs and their uptake by other blockchain protocols imply a changing market dynamic, indicating an escalating consumer inclination towards this technology.

1.3. **Added Value**

The prevalence of the advertise-based internet model has ingrained the belief that all online content should be freely accessible. Digital content, whether it be tweets, memes, videos, articles, or anything else, is generally expected to be free of charge; otherwise, most users tend to dismiss it. This attitude complicates understanding why someone would purchase a digital asset, such as an NFT, which is ostensibly free to view and reproduce. The question, "Why would I want to buy something that anyone can view online, take a screen capture, and then claim 'ownership' of the digital result?" encapsulates this dilemma of paying for what is perceived as free content.

Nevertheless, it offers an appropriate representation of how collectibles can appreciate, potentially exceeding their initial worth significantly. Though rarity is not the sole determinant of value, several factors influence the valuation of collectibles.

The term "provenance" denotes an item's historical background and origin, particularly in collectibles. This concept serves as a form of validation for collectibles, providing a record of ownership that vouches for the authenticity and quality of the item. The provenance of an art piece is a comprehensive chronicle of its owners, tracing its journey from the artist to the current holder. Provenance plays a crucial role in transactions involving art and collectibles, substantially influencing the sale's success.

The value of a collectible can be influenced by its historical background and the timeline of its creation. A case in point is the rare pennies minted in 1943 and 1944, whose existence resulted from inadvertent production during World War II. These coins hold a distinctive appeal, setting them apart from others minted erroneously. This illustrates that the historical narrative associated with a collectible can significantly influence its valuation.

A collector's emotional bond with a collectible can significantly influence its perceived value. This personal sentiment can occasionally lead collectors to invest more in a particular item due to its importance.

The state of preservation of a collectible significantly influences its market value. This is why every collectible undergoes a meticulous examination to assess any signs of damage or decay, with a grade assigned reflecting its current condition. However, this factor might be less significant for unique, one-off pieces. For collectibles with multiple copies, like the wartime penny, the correlation between condition and value is clear superior condition yields higher value. Consequently, collectors typically put significant effort into preserving their collections.

Owning a comprehensive collection of all variations of a specific collectible significantly influences its worth. For avid collectors, the thrill lies in obtaining every available piece. The rarer the collectible, the more challenging it is to possess an entire collection, enhancing the value of individual components and the overall appeal on the market.

The interaction between supply and demand, propelled mainly by collectors, is the primary determinant of a collectible's value. Nevertheless, other contributing factors include the object's condition, provenance, sentimental attachment to the collector, and the exceptional quality of owning a complete set. Authenticity is a paramount aspect of collectibles' value, and the conventional art and collectibles sectors have been consistently challenged by issues surrounding counterfeits, forgeries, and questions about authenticity.

The art sector has long been wrestling with the problem of counterfeit art, a concern that persists to the present day. According to an investigation by Switzerland's Fine Art Expert Institute in 2014, an estimated half of the fine art circulating in the market was either fraudulent or misidentified. Despite disputes regarding this percentage, new cases of counterfeit art are continually discovered in private collections, galleries, and internationally renowned museums. Nevertheless, the global art market exceeded $38 billion in total sales in 2019.

In the conventional sense, art authentication heavily depends on the subjective judgments of specialists, referred to as connoisseurs. This method, however, is susceptible to human inaccuracies, predispositions, and the potential for dishonest practices. These issues become increasingly concerning when dealing with high-stakes art transactions involving substantial monetary values. Moreover, the elite nature of the high-end art community often acts as a barrier to entry for those outside the group. Consequently, the subjective reliance on "experts" for authentication in the art world puts billions in value at risk, raising uncertainty about the prevalence of unidentified forgeries and the reliability of the authentication process.

The artwork's authenticity is also identified through its chain of ownership, or its provenance, which presents a documented ownership history from the present owner to the initial artist. However, this lineage might need to be more present or even fraudulently manipulated in instances of forgeries. This concern is rampant within the art sphere, casting doubt on the authentication process, especially when it involves transactions of significant financial magnitude.

Furthermore, instances of art forgers introducing fabricated provenances into the records of prestigious institutions, such as the Tate Gallery, the Victoria and Albert Museum, and the British Council, only intensify the concerns about the reliability of these archives.

The worldwide market for collectibles is expansive and believed to be valued at approximately $370 billion, comprising many items, including but not limited to sports keepsakes, historical artifacts, comic books, postal stamps, and various types of coins. Nevertheless, the market is fraught with duplications and illicit copies, with estimations suggesting that as much as 80% of antiques transacted online could be illegally obtained or counterfeit. Historically, about 90% of the sports memorabilia traded in the United States was suspected of being falsified, prompting interventions from the Federal Bureau of Investigation against the proliferation of fake items.

The problems of authenticity and provenance that traditional art and collectibles suffer from can be solved using NFTs, which also offer several other benefits.

NFTs bypass the need for expert validation, which is common in traditional art since their authenticity can be confirmed via blockchain technology. The genuineness of an NFT can be quickly established by inspecting its smart contract address using a block explorer tool. The block explorer exhibits both the NFT's address and the originating address. If these details correspond with the recognized address of the artist or creator, the NFT is deemed genuine. Platforms for trading NFTs, like OpenSea, provide options to verify an NFT's creator by examining the Trading History section of the NFTs. If the creator's name or address aligns with that of a verified artist or creator, it is considered an authentic NFT. There is no dependence on experts or conjecture; the validation process is direct and built on blockchain principles.

The lineage of NFTs is defined through a succession of ownership that begins with the creator and culminates with the present owner. This feature of NFTs is facilitated by blockchain validation, a core characteristic of all cryptocurrencies.

As will be detailed further, each transaction on the blockchain is subject to validation. Validators, also known as miners, can authenticate transactions within a block using methodologies such as proof-of-work or proof-of-stake. Validators ensure that the address initiating the cryptocurrency transaction possesses the requisite funds. This involves examining the transaction lineage starting from the present block, tracing it back through various wallets, and ending at the most recently authenticated block. This process confirms the transaction's inception in the blockchain's genesis block. The intricate details of every NFT, from its creation, and line of ownership to its transaction history, are indelibly recorded on the blockchain. This information can be accessed by anyone who searches the NFT's address on a block explorer or checks its transactional past on a marketplace. Given the irreversible nature of blockchain technology, a secured and immutable provenance is guaranteed.

Blockchain technology ensures the perpetual preservation of NFTs. In contrast to tangible collectibles, NFTs remain unaffected by decay or accidental damage. Nevertheless, akin to physical artworks and collectibles, NFTs can be purposely destroyed in a process referred to as "burning."

The duplication of a cryptocurrency, such as Bitcoin, would render it valueless due to the fact that its worth is derived from its limited availability.

Replicating Bitcoin or any other form of cryptocurrency, including NFTs, is not feasible. This is primarily because NFTs, similar to all other forms of cryptocurrency, have a supply that is controlled and guaranteed by blockchain technology, making any attempt at duplication unachievable. Therefore, the limited availability of NFTs is safeguarded in this manner.

Blockchain technology guarantees that NFTs are both scarce and genuine, giving digital artists the confidence to sell their creations without the anxiety of encountering fraudulent replicas. This paves the way for a novel and profitable digital art and collectibles market, a previously nonexistent market currently generating millions of revenue.

When a creator sells an artwork, they receive solely the payment from the original sale. If that artwork is resold at a more excellent price, the original artist does not receive a portion of the gained profit nor any profit from future transactions. The system lacks a recurring royalty mechanism that would allow the artist to capitalize on the appreciation of their work, barring the production of new pieces.

In contrast, NFTs usher in an unprecedented marketplace for digital art and collectibles, affording artists the opportunity to partake in future sales via built-in royalties. In stark difference to traditional art transactions, NFT royalties are seamlessly transferred to the artist's cryptocurrency wallet, circumventing the need for invoicing, tracing or third-party involvement. However, it is imperative to note that perpetual royalties are only ensured if the NFT is traded in the same marketplace where it was initially minted.

NFTs utilize the advantages inherent to the decentralization feature of blockchain technology.

Centralized transactional systems, such as banking institutions, despite their numerous branches, operate based on a single source for their database and transaction validation process. They hold control over their databases and the verification of all associated account transactions.

Centralized systems bear the vulnerability of data accumulation in a singular location, rendering them susceptible to malicious cyber-attacks. A security breach could lead to unauthorized access to sensitive data or alterations of the records. This vulnerability was evident during the 2019 security breach at Capital One, where the attacker leveraged a singular point of weakness to gain unauthorized access to the personal data of over 100 million individuals.

Decentralized systems, on the other hand, provide a robust defense mechanism against hacking with no single point of vulnerability. This complexity makes it significantly difficult for an attacker to modify the database. For instance, with Bitcoin, should an attacker attempt to modify past transactions or add fraudulent transactions to the blockchain through a single node, the other nodes within the network would identify these irregularities and reject the alterations.

Centralized systems like banks have complete control over their database and transaction processes, including the ability to hold funds subject to government regulations. This central authority has the power to dictate the management of the database and control the transaction process, including holding funds for a specific period. There is little opportunity for individuals to make changes in these circumstances.

2. State of the art

2.1. **Characteristics**

While there may be variations and different standards for NFTs, some widely accepted and fundamental characteristics are common to most NFT deployments. These characteristics include uniqueness, transparency, verifiable ownership, programmable assets, and unalterable records.

One key characteristic of NFTs is their uniqueness. NFTs can be produced in limited quantities, with each token being individually identifiable. For example, CryptoPunks issued 10,000 unique NFTs. Similar NFTs may sometimes exist, such as numbered series of an artist's digital work. This uniqueness can be considered in the analogy "one out of X," where each NFT is unique within its series.

A rarity in the context of NFTs can take many forms and be divided into three categories: artificial, numerical, or historical. Artificial rarity refers to the uniqueness of an NFT as determined by its code or the conditions of its issuance. For example, Cryptopunks have varying levels of rarity based on their specific features. The rarity of a punk with a Medical Mask is determined by the fact that only 1.75% of Cryptopunks have this feature, making them rarer than those with an Earring, which has a 24.59% chance of appearing. Numerical rarity refers to the limited number of a particular NFT, while historical rarity is based on the NFT's past, such as its creation date or unique history.

Numerical rarity is closely connected to artificial rarity and is, therefore, easy to understand. For example, suppose a famous artist releases 100 digital copies of their latest album as NFTs. In that case, those 100 copies with the artist's "digital signature" will be more scarce and, therefore, rare than simply streaming the album on Spotify. This can be thought of as analogous to owning a physical album that is signed by the artist versus one that is not.

Finally, historical rarity refers to the historical significance of an NFT. This can take many forms. For example, the crypto punks are considered historically rare because they were some of the first generative NFTs ever issued. Additionally, since blockchains record an immutable history of ownership, some NFTs might be historically significant because they were owned by notable entities or individuals.

Proof of ownership, the potential for fractional ownership, and provenance tracking are all essential characteristics of NFTs that are backed by real-world tangible assets. These features enable the verifiable ownership of the underlying assets, the ability to hold partial ownership of the assets, and the ability to track the history of the assets.

Immutability is a fundamental property of all blockchain-based tokens, including NFTs. This means that the tokens and the information embedded in them are highly resistant to tampering unless the underlying blockchain protocol is compromised. This creates a high level of trust and transparency in the system.

The feature of programmability is frequently highlighted as a distinguishing factor that sets NFTs apart from tangible assets. Apart from facilitating creative or commercial endeavors, NFTs can be programmed in line with any software application. This can be employed to guarantee that artists receive ongoing royalties or moral rights over the lifespan of a piece rather than merely at the point of initial sale. Furthermore, pioneering applications have showcased how NFTs can serve as collateral in numerous decentralized finance (DeFi) platforms, akin to the role of a mortgage in conventional finance.

2.2. **Anatomy**

This chapter presents a comprehensive outline of the economy emerging around NFTs. With a focus on the participants within this ecosystem and the elements, they engage with.

Users

NFTs are frequently utilized for the sale of digital artifacts such as images, audio files, and videos. Participants in the NFT ecosystem typically fall into one of three roles: content creators, sellers, and buyers. Initially, digital content is developed by creators and uploaded to hosting services (external entities) to allow public access. However, when it comes to the sale of the content, specific creators lack the technical prowess to convert their art into an NFT and place it on the blockchain as a token. As a result, they delegate the responsibility of minting NFTs to sellers, who then list them on marketplaces. In some instances, the roles of the content creator and seller are performed by the same individual. Once the NFTs are displayed on a marketplace, potential buyers can purchase the artwork at the listed price, submit offers, or participate in bidding. If their offer is accepted or they emerge victorious from an auction, the ownership of the NFT is transferred from the seller to the buyer, a process carried out by invoking the transferFrom() method.

Marketplaces

NFT markets (NFTMs) are decentralized application (dApp) platforms that facilitate the exchange of non-fungible tokens (NFTs). Typically, an NFTM comprises two main components: a user interface that interacts with the web and a series of smart contracts that connect with the blockchain. Users interact with the web application, which transmits transactions to the smart contracts on their behalf. There are two main types of contracts:

- marketplace contracts, responsible for implementing the NFTM protocol's functionalities related to blockchain interaction
- Token contracts, which govern NFTs.

Marketplaces commonly allow the following actions: user identification, token creation, token listing, and token trading. The collective term for these token-related activities is "events." Depending on where these events are stored, there are three general categories of NFTM protocol design:

- On-chain: All events occur directly on the blockchain. This design is costly for users since every action incurs a gas fee. NFTMs such as Axie, CryptoPunks, Foundation, and SuperRare use this design.
- Off-chain: The events are stored in a centralized, off-chain database overseen by the NFTM. This design is gas-friendly since users interact with the web app rather than the blockchain to conduct a variety of tasks. An excellent example of an off-chain NFTM is Nifty.
- Hybrid: Based on their kind, events are either off-chained or on-chained when stored. On-chain and off-chain events are linked together using a cryptographic check to guarantee the integrity of the process. This model is used by Rarible and OpenSea.

User authentication

To avail of the services offered by Non-Fungible Token Marketplaces (NFTMs), individuals must first complete a registration process. Once registered, they can opt for one of two authentication workflows: traditional credentials-based (username and password) or signature-based authentication. The latter workflow initiates with the user signing a challenge string. Subsequently, the marketplace retrieves the user's address from the elliptic-curve signature. Platforms like OpenSea, Rarible, Foundation, CryptoPunks, and SuperRare operate using this model. Considering the unique nature of Ethereum private keys, this authentication technique typically offers higher security compared to traditional passwords, which are generally derived from a restricted character set, shorter, and more susceptible to brute-force attacks.

Token minting

A token is produced by invoking a suitable method in the token contract, which typically adheres to the ERC-721 or ERC-1155 standards. A single token contract can oversee the ownership of multiple NFTs. Each NFT is allocated a unique integer known as a tokenId. As such, a specific NFT can be identified on the blockchain by its unique pair of token_contract_address and tokenId. A 'collection' refers to a group of NFTs that share common characteristics or are related by a specific theme.

The process of minting an NFT can take different forms:

- Default contract: As part of a pre-deployed, specified token contract managed by the marketplace, the token is created. When creators do not deploy a custom contract, marketplaces like OpenSea, Foundation, and SuperRare offer a default contract for holding NFTs.
- Replica contract: The NFTM initiates a contract on behalf of the creator to manage the collection to which the NFT belongs. The contracts deployed have identical bytecode but can be personalized via initialization parameters. Nifty and Rarible are examples of such NFTMs. Since both default and replica contracts are managed by the NFTM, they are collectively referred to as internal token contracts.
- External contract: The creator independently deploys a custom contract to manage the collection and later imports it to the marketplace. For compatibility with NFTMs, external contracts must comply with a well-established token standard or custom integration is required. OpenSea and Rarible allow external contracts on their platforms.

One token contract can oversee one or more collections. Generally, replica or external contracts manage a single collection, whereas the marketplace default contract handles multiple collections. In the latter scenario, the NFTM dApp maintains an off-chain association between the set of token IDs and their respective collections.

Token listing

Once created, a seller lists their assets for sale. To list an NFT on a platform, some NFTMs, e.g., Foundation, SuperRare, and Nifty, mandate the seller or the entire collection (the NFT is a part of) to be verified. Even for the NFTMs where verification is optional, for example, OpenSea, and Rarible, getting an artist or a collection verified provides credibility and increases buyers' confidence. NFTMs display special badges on verified profiles of artists and collections, which helps build a brand, and receive preferential treatment to boost sales, such as search priority and safe-listing to suppress safety-related alerts before the purchase.

Token trading

Purchasers have the ability to either place bids or make offers on available assets. Once a bid is accepted or an auction concludes, the non-fungible token marketplace (NFTM) facilitates the transfer of assets from the seller's account to the purchaser's. This transfer typically triggers a service fee charged by the NFTM. The bidding mechanism of an NFTM can be characterized by the following key elements:

- Pricing strategy: Prices can either escalate or decrease with each bid. In English auctions, the bidding starts at a reserve price, i.e., the lowest price a seller is willing to accept for an NFT. The buyer's subsequent bids incrementally raise the price, with the highest bid ultimately securing the NFT. This approach is adopted by many NFTMs, such as OpenSea, Foundation, and SuperRare. Conversely, Dutch auctions initiate bidding at a high price point, which is subsequently lowered by the seller. The NFT is awarded to the bidder who first accepts the reduced price. Platforms like Axie follow this model.
- Bid storage: Bid records can either be stored on-chain (as seen with CryptoPunks, Foundation, and SuperRare) or off-chain (such as Nifty, Rarible, and OpenSea). Some protocols, like Wyvern (used by OpenSea), retain both sell orders and bids off-chain for improved gas efficiency, though the order matching and NFT transfer occur on-chain. This prevents manipulation from a malicious buyer by ensuring cryptographic verification of the buy order against the corresponding sell order.
- Active bids: Some NFTMs, like CryptoPunks, Foundation, or SuperRare, do not permit multiple active bids on the same asset. When a new bid surpasses the highest current bid, the outbid party is automatically refunded.
- Bid withdrawal: Some NFTMs allow bidders to withdraw their bids, such as CryptoPunks, while others, like Foundation, do not provide this option.
- Bid settlement: In most instances, the seller's intervention is not required for bid settlement—the asset is automatically transferred to the highest bidder. However, some NFTMs like CryptoPunks require explicit acceptance of the bid by the seller.

A sale conducted by someone other than the original creator is classified as a secondary sale. A predetermined fee, referred to as a royalty, is provided to the creator from every secondary sale. The royalty percentage is specified by the creator before the initial (primary) sale. The designated amount is then subtracted from each subsequent sale and credited to the creator. The deduction process can be either on-chain, where the marketplace contract determines the royalty during the purchase transaction, or off-chain, where the NFTM application monitors the accumulated royalties from all transactions.

There are also external entities, outside the purview of both NFTMs and the blockchain, that offer critical infrastructure for the system's operation. For instance, creators might store their artwork on web servers or storage services like Amazon S3 or IPFS. Purchasers of the NFT can demonstrate their ownership by showcasing the artwork on photobook-style websites or digital NFT photo frames. These websites, photo frames, and NFTMs retrieve tokens from the blockchain and the corresponding artwork from these services.

2.3. **Use-Cases**

Gaming

The gaming industry's collectibles segment stands to be revolutionized through the application of Non-Fungible Tokens (NFTs), a technology that's gaining significant traction in the gaming sphere. Digital games echo physical games and collectibles in many respects, yet their digital constitution permits increased adaptability and prospects. NFTs can intensify the attributes of digital games and offer avenues for innovation. Freed from the physical world's constraints, such as material degradation or geographic restrictions for players, NFTs operate exclusively in the digital domain.

Items found within digital games often hold substantial value for players due to a multitude of reasons. These items can symbolize a player's commitment in terms of time and resources or serve as a testament to their prowess. Mirroring physical collectibles, these in-game items can bear intrinsic value to players. Moreover, digital collectibles' trade ability and potential for liquidity enhance their perceived worth even further. The realm of digital collectibles also provides artists with a platform for broader creative expression, leading to a more diverse array of artistic styles and designs.

In conventional digital games, the features and utilization of items are identical for all players. These items are differentiated using a unique identifier, typically stored on a central server. However, blockchain technology introduces a decentralized approach to this information storage. Unique identifiers of in-game items can be represented as NFTs and minted on the blockchain, bolstering the security and decentralization of in-game assets.

Gamers often amass in-game items through extensive gameplay, essentially owning these items within their personal accounts. Nevertheless, the ultimate control over the items and account information rests with the game provider, causing the value of these items to be confined within a centralized system. Therefore, when a player ceases to play the game, the inherent value of their in-game items dissipates without yielding any financial returns. Blockchain technology offers a solution to this problem by enabling the tracking of ownership through transactions on a distributed ledger, enhancing transparency and security related to the possession of in-game assets.

The transformation of in-game items into tokens and monitoring their ownership via blockchain could potentially bring about a significant change in the gaming sector. In the past, games typically involved players investing money for playtime, with enjoyment being the sole return. However, the advent of NFTs and blockchain technology has opened up the opportunity for players to monetize their gaming hours by selling their tokenized assets on a marketplace. This shift has given rise to the concept of "play-to-earn", signifying the ability to accumulate cryptocurrencies through gameplay. Games like Cryptokitties, Splinterlands, Axie Infinity, Aavegotchi, and LiteBringer have prominently adopted the NFT model.

Cryptokitties, launched in 2017, emerged as one of the pioneers in gaining mainstream recognition. The game is based on the Ethereum blockchain and allows users to breed and trade digital cats using NFTs (ERC-721). The price of these cats is regulated by the marketplace's supply and demand dynamics. The success of Cryptokitties was immense, contributing to 25% of Ethereum's network traffic through its transactions.

Axie Infinity, a game that utilizes NFTs, is a popular offering built on the Ethereum blockchain. Drawing inspiration from Pokémon, the game enables players to breed, raise, and engage in battles with digital pets. The game also introduces a digital land system, where each plot of land corresponds to an NFT. By August 2021, Axie Infinity's daily active players had reached a million, testifying to its widespread appeal.

Aavegotchi represents another game leveraging the Ethereum blockchain, featuring pixelated ghosts. It adopts the ERC-721 standard for generating NFTs and gives players the ability to stake their NFTs, subsequently earning token interest used in the AAVE protocol. This distinctive amalgamation of Decentralized Finance (DeFi) and NFTs is a defining attribute of the game.

Splinterlands, a card game platform established in 2018, employs blockchain technology to facilitate the exchange of in-game cards. The platform operates on the Hive blockchain, storing only actions on the chain, which occasionally leads to a slowdown in the user experience. In July 2021, the platform successfully garnered $3.6 million through a private token sale.

LiteBringer, an idle role-playing game, allows participants to advance characters from various categories, such as wizard or warrior. The game's architecture is built on the Litecoin blockchain, with player actions, including character creation or embarking on quests, incurring gas fees as they're logged as transactions on the blockchain. A gaming industry data aggregator, currently monitoring 5211 games with issued NFT collections, provides real-time insights into blockchain game usage and offers a comprehensive classification system based on the game's genre.

A recent development in the blockchain gaming sector has seen a rapid increase in interest in start-ups operating within this niche. The model known as "play-to-earn" grants gamers the ability to possess and possibly accrue value from assets within a gaming environment. As users contribute to the in-game economy, they generate value for both fellow players and game developers, receiving rewards in the form of metaverse assets for their participation. These digital assets could range from cryptocurrencies to in-game elements that have been tokenized on the blockchain.

The primary benefit of the play-to-earn business model is the continuous value generation with the potential for monetization by gamers. Regardless of whether a gamer invests financially in gameplay, the items they collect retain resell value. In contrast, conventional gaming platforms such as Fortnite and League of Legends generate significant revenue from players purchasing digital skins that lose their value when the player ceases gaming, thereby leaving the players without any return on their expenditure. The play-to-earn paradigm, on the other hand, offers players the chance to recover a portion of their investment even after they cease active gameplay.

Art

NFTs have gained popularity in the digital content sector, especially due to their inherent diversity. Presently, digital art is the most prevalent application of non-fungible tokens, with their worth stemming from the unique digital authenticity and ownership they provide. The digital replication and distribution of art have posed significant obstacles to the successful digitization of art, given the ease with which digital files can be duplicated, shared, and circulated. Formats like JPG, which are entirely interchangeable and bear identical metadata, make it challenging to assure exclusivity and permanence in digital art ownership. NFTs, however, enable the production of limited editions, thereby introducing the concept of rarity and consequently, value. Digital artists are now capable of selling their creations, enjoying the same advantages that artists of physical works have been privileged with for centuries. Platforms for NFTs allow artists to engage directly with prospective purchasers, circumventing conventional galleries and auction houses. The expansion of the NFT art market has led to the emergence of a novel trend: hybrid galleries exhibiting distinct pieces of non-fungible art. As reported by CoinTelegraph, a minimum of nine NFT galleries and exhibitions have been launched this year.

NFTs of experiences of museum artifacts

The rising value and interest in NFTs in the realm of art have led museums to consider the potential integration of these digital tokens into their operational procedures. The restrictions placed on indoor assemblies due to the pandemic have posed a significant challenge for many museums, leading to a significant decrease in visitor numbers. Digital marketplaces can present these institutions with an alternative revenue source by offering NFTs for auction. Moreover, by making NFTs publicly available, museums could potentially boost audience engagement and interaction, thereby diminishing their dependence on generous donations from affluent individuals.

In 2017, the National Museum Liverpool in the UK initiated a project titled 'Crypto Connections'. This project enabled museumgoers to form NFTs encapsulating their interactions with specific museum exhibits. Due to the lack of alternatives for generating NFTs at the time, these tokens were formed on the Ethereum blockchain. The project's primary objective was to cultivate a feeling of communal ownership and mutual stewardship over digital collections. This approach allowed spectators to gain deeper insights into an object by viewing others' perceptions and evaluations of it. An illustrative example could be understanding the significance of a jar being displayed in a museum. If an NFT chronicles the history of the object and subsequent viewers contribute their personal experiences with the object over generations, the NFT can surpass the physical object itself in terms of interest.

One potential future use case for this kind of NFT is with statues. Instead of demolishing controversial statues, an NFT could be attached to the statue to provide context and history, allowing viewers to better understand the reasons for the statue's controversy. Another potential use case is the curation of digital art galleries and museums. Transporting priceless artifacts is a major undertaking, but transporting and curating digital versions of these artifacts as NFTs allows more people to enjoy and appreciate them. In addition, the enhanced viewer experience allows for a greater appreciation of the inherent value of the artifact.

Supply Chain

The supply chain and logistics industries are sectors that could benefit from the use of NFTs. Like any technology, NFTs aim to address some of the challenges in these sectors. One challenge that brands face is the authenticity of their products. A brand's reputation is an intangible asset that carries a lot of value for businesses. For example, distilleries may be known for producing specific wines. NFTs can be used to create digital twins of bottles on the blockchain, allowing for real-time tracking and verification of authenticity. Platforms that provide this service include WiV and TATOO, developed by consulting firm EY.

Secondary markets, where transactions take place between individuals, are another area where NFTs can be useful. Item collectors are often participants in these markets, but it can be difficult and costly for buyers to verify the authenticity of the products they are purchasing. NFTs can provide real-time verification of authenticity, helping collectors and consumers combat forgery. Nike has even secured a patent for a project called "Cryptokicks" that uses NFTs to store the unique identifier for each pair of shoes.

An integral facet of logistics is the matter of goods ownership. In our globalized economy, tracking ownership often involves complex documentation and necessitates considerable involvement from numerous parties, including carriers and storage facilities. Non-fungible tokens (NFTs) on the blockchain can potentially streamline this process by generating a digital duplicate of the item and noting its transactional lineage on the blockchain. This is the methodology employed by the Ownest Initiative in the realm of supply chain management.

While some applications use the blockchain as a transactional data repository, this method can be susceptible to false data declarations by those involved in the supply chain. The Ownest initiative counters this drawback by utilizing NFTs to monitor ownership and responsibilities related to tangible products. The initiative has devised two unique token standards, termed Unitary and Stock tokens, that are comparable to the Ethereum blockchain's ERC-721 and ERC-1155 standards.

Music Royalties

In the realm of music, NFTs can be utilized to forge unique collectible music pieces, facilitating equitable distribution of royalties and endorsing novel crowdfunding methods for music creation. Furthermore, NFTs employed on blockchain-enabled streaming platforms can accurately account for the revenue produced by a specific track, yielding a transparent avenue for musicians to distribute their work. Start-ups like Audius, having embraced this technology, have seen a surge in their user base, recently reaching six million users. Nevertheless, the challenge lies in contending with well-established music streaming giants such as Apple Music, YouTube, and Spotify.

Authorization (Keys/access control)

Once a user is verified, IT systems frequently use authorization processes to regulate access to resources. This includes assessing a user's access permissions according to a set of guidelines and then deciding to either permit or refuse access. Traditional tokens are commonly employed to symbolize the entitlement to access resources. However, NFTs can also fulfill this role, providing enhanced security. For instance, tokens are used in the OAuth2.0 authentication standard, and studies by authors such as Esposito et al. and Fotiou et al. have explored the use of NFTs in this scenario.

Given their uniqueness and the ability to precisely control their scarcity, NFTs can be employed as keys to unlock physical doors or digital wallets. This introduces an additional level of access control, limiting access to only those in possession of the corresponding NFT. This application could also be extended to event ticketing.

Identity

In the modern digital era, personal identity is progressively transitioning from identity-focused systems to reputation-focused systems, with users adopting pseudonyms. Nevertheless, these individuals maintain their uniqueness within a given ecosystem. Non-fungible tokens (NFTs) can store particular metadata that links an individual's physical world identity with their digital identity, providing unique privileges solely to the owner of a specific NFT. This also allows for the enablement of permissioned multi-signature functionalities made achievable through NFTs.

Point system
Frequently, NFTs are leveraged to acknowledge accomplishments within games or specific environments. This includes team appreciation NFTs, reward NFTs, or evidence of participation NFTs. An instance of this would be the Proof of Attendance Protocol (POAP) that utilizes xDai to develop NFTs for this aim. Additionally, Decentralized Autonomous Organizations (DAOs) commonly use NFTs to signify specific user wallets according to their involvement and contribution to the DAO. This method can be employed to remunerate or reward the most engaged user wallets based on their NFT holdings.

2.4. **Storage**

When an NFT for digital art is acquired, the blockchain registers the transaction, officially acknowledging your ownership. However, the actual content of the NFT isn't stored directly on the blockchain and instead relies on off-chain storage solutions, primarily trusted cloud storage providers or the InterPlanetary File System (IPFS).

IPFS is generally favoured for NFT storage due to its decentralized nature. This system stores content across various locations, enhancing its security. On the other hand, trusted cloud storage providers, such as Google Cloud or AWS, offer reliable services, although the safety of the content is contingent on the ongoing payment of storage fees by the hosting organization.

Potential risks associated with losing NFT content should be factored in, especially in scenarios where the marketplace or cloud storage provider ceases operations or discontinues paying the requisite fees. With IPFS, the content is expected to remain secure as long as the network is maintained. Furthermore, other decentralized storage alternatives like Arweave have gained prominence in the market.

The manner in which NFT content is stored presents a critical challenge, as it contradicts one of the fundamental tenets of blockchain technology, which is the elimination of reliance on a trusted third party. For instance, an individual like an artist can create an NFT and store its content on a private server, but if that server becomes inaccessible, the content disappears. Such a lack of decentralization is far from ideal, as it compromises the trustless, peer-to-peer transactions that are the cornerstone of blockchain technology. Although certain decentralized solutions like IPFS are more compatible with blockchains, marketplaces frequently resort to centralized storage platforms due to their simplicity and cost-effectiveness.

The preservation of unlockable content, such as visuals or multimedia, is a significant issue. For instance, on platforms like OpenSea, only textual data can be included as unlockable content, requiring images or videos to be stored on external online platforms. If the NFT's creator ceases to sustain their web or cloud storage platforms, the associated media may be lost. This underscores the necessity for a more robust and secure method of preserving NFT content.

NFTs reside on a blockchain, a type of decentralized and distributed database that keeps an expanding series of records known as blocks. Every block encompasses a timestamp and a reference to the preceding block, forming a blockchain. This arrangement enables the upkeep and updating of the database in a decentralized way, eliminating the need for a central governing entity.

A digital wallet capable of accommodating and managing NFTs is required for their storage. A majority of digital wallet providers cater to NFTs, with several offering specialized wallets specifically designed for this use.

Upon obtaining a digital wallet, your NFT can be stored by directing it to its distinctive address. This action records the NFT on the blockchain, where it is securely kept on the network until you opt to either transfer it or sell it. The significance of employing the InterPlanetary File System (IPFS) for NFT storage lies in the distribution of data rather than it being housed on a singular server, thereby making it more challenging for potential hackers to locate and breach the NFTs. With data dispersed across numerous computers on the network, it enhances resilience against interruptions or assaults. In a scenario where one computer is offline, data remains accessible from other nodes within the network.

For the purpose of enhancing your digital wallet's security and the safety of your NFTs, it is crucial to adhere to optimal cybersecurity practices. These include the utilization of robust and unique passwords, activation of two-factor authentication, periodic updates of your wallet software, and vigilance against phishing attempts or dubious links.

By integrating these security protocols and employing IPFS for NFT storage, you can effectively safeguard your digital assets. It's worth stressing that the security of your digital wallet is of utmost importance since anyone with access to it can manipulate your NFTs.

Utilizing the InterPlanetary File System (IPFS) alongside blockchain technology can enhance the efficiency of NFT storage. This method facilitates the distribution of NFT data across numerous networked computers instead of relying on a single central server, enhancing the system's resistance to potential disruptions or cyber-attacks.

IPFS

The Interplanetary File System (IPFS) is a protocol and decentralized network that allows for data to be stored and transferred within a distributed file system. In IPFS, a file is defined and addressed based on its specific location. The content identifier in IPFS is a cryptographic hash of the content found at a designated URL ("/ipfs/"). Since the URL is derived from the file's content, links within IPFS cannot be altered. Through the hash functions of content identifiers, users are able to verify the integrity of a file, confirming that there have been no changes since its initial publication (IPFS, n.d.).

While IPFS presents a possible solution, it comes with several challenges. Firstly, file sharing under IPFS relies heavily on traditional communication channels such as messaging, emails, and other social media platforms. This mode of sharing can increase the risk of layer-8 vulnerabilities, fostering the propagation of harmful links. Secondly, the process of file discovery can be cumbersome and unsatisfactory for users, thereby adversely affecting the marketplaces' business reputation and resulting in data loss from nodes. Certain centralized services, such as Pinata, offer support with pinning these files. However, integrating two systems could prove complex and cost-intensive, particularly for smaller marketplaces lacking an adept technical team.

URI

A URI, or Uniform Resource Identifier, is a string of characters used to identify a name or a resource on the Internet. URIs can be either URLs (Uniform Resource Locators), which specify the location of the resource, or URNs (Uniform Resource Names), which identify the resource by name.

For example, a URL might be something like "https://www.google.com" which specifies the location of the Google website. A URN might be something like "urn:isbn:0-486-27557-4" which identifies a specific book by its ISBN number.

URIs are used to identify and locate resources on the Internet, and they are an essential part of the way the Internet works. URIs are used in a variety of contexts, including the identification of web pages, files, and other resources, as well as the identification of services and protocols on the web.

2.5. **Marketplaces**

Utilizing information from dappradar.com, I've pinpointed the leading five NFT marketplaces, determined by the number of wallets used and the aggregate volume in US dollars. These marketplaces have been ordered according to these specific criteria.

OpenSea

OpenSea.io, established in 2017, is recognized as the industry's foremost NFT marketplace, boasting the most significant quantity of NFTs and the highest sales volume in the sector. The platform currently hosts an impressive 15.5 million NFTs and has recorded a staggering $354 million in sales. It is appreciated for its user-friendly design and simplicity, which makes it an excellent choice for those new to the world of NFTs. OpenSea provides an extensive array of NFTs for collectors, including a variety of digital asset categories, such as:

- Digital Art
- Collectibles
- Music
- Domain Names
- Virtual Real Estate
- Digital Trading Cards
- Virtual Gaming Items

Pros

- Largest NFT marketplace.
- Easy to create, sell, and buy NFTs.
- Free to mint NFTs.
- Only a one-time double gas fee to list NFTs for sale.
- Fee of only 2.5 percent of sales.
- Various blockchain systems such as Flow, Tezos, and Binance Smart Chain.
- Artists can set their royalties.

Cons

- Can buy and sell NFTs only with cryptocurrency.
- Based mainly on the Ethereum blockchain, which can have high gas prices for transactions.
- Accommodating files up to 100 MB in size.

Rarible

Website: Rarible.com

Rarible.com is an accessible NFT marketplace designed to facilitate the generation, trading, and acquisition of various types of NFTs owned by a Decentralized Autonomous Organization (DAO). It features an intuitive interface, making it straightforward for users to navigate. To foster user involvement, Rarible has incorporated elements reminiscent of social media platforms, such as following NFT creators and receiving alerts when new NFTs are launched. The platform has also introduced its proprietary token, RARI, which acts as a governance tool on the platform and incentivizes active participants by granting them influence over the platform's future development. Rarible imposes a 5% commission fee on every transaction, which is equally divided between the buyer and seller at 2.5% each.

Pros

- Easy to create, sell, and buy NFTs
- Vibrant community

Cons

- Can buy and sell NFTs only with cryptocurrency.
- Based on the Ethereum blockchain, which can have high gas prices for transactions.
- Must pay a gas fee every time you mint.
- maximum file size of 30 MB.

SuperRare

Website: Superrare.com

SuperRare operates as a unique NFT marketplace, focusing on offering one-of-a-kind digital art NFTs. This platform presents a fresh approach for individuals to interact with art, culture, and the practice of collecting online. Boasting a robust community, SuperRare maintains a log of prominent collectors and celebrated artists. Resembling an elegant art journal, its well-structured website showcases a daily collection of articles related to digital art.

Pros

- Rare, single-edition NFTs
- Easy and intuitive to use
- Strong community

Cons

- Fee of 15 percent of primary sales.
- Need to apply to sell NFTs.
- Based on the Ethereum blockchain, which can have high gas prices for transactions.

Foundation

Website: Foundation.app

Foundation positions itself as a platform tailored for the exhibition of work by artists, curators, and collectors. Its design aesthetic takes significant cues from social media platforms, particularly Instagram, and it encourages users to associate their social media profiles with their Foundation accounts. Although registration on the platform is open to everyone, selling NFTs requires community endorsement through upvotes. This community-based vetting process, despite introducing a level of difficulty to NFT selling, guarantees that only high-quality artwork is displayed also linked to the distinctive sales model mandates that a reserve price must be reached to initiate a 24-hour auction.

Pros

- Nice variety of quality art NFTs.
- Active community of artists and collectors.

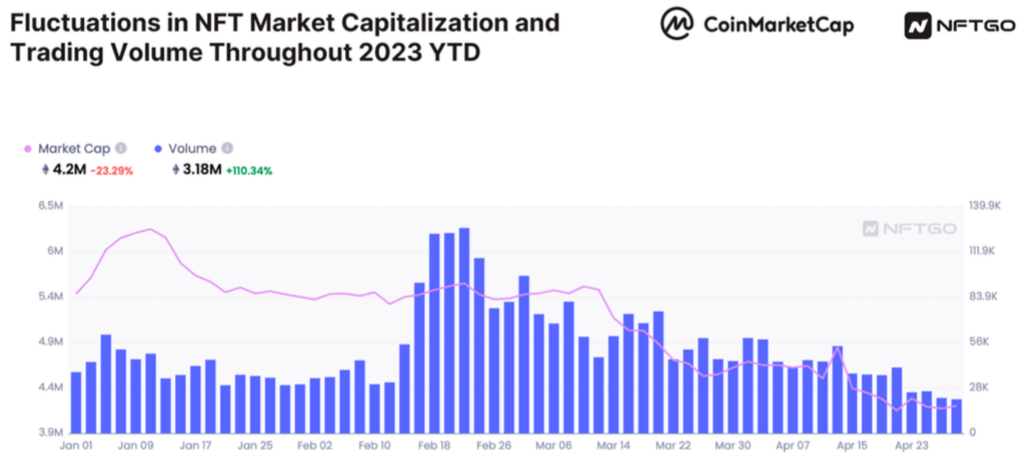
Cons

- Fee of 15 percent of primary sales.
- No way to filter searches.
- Based on the Ethereum blockchain, which can have high gas prices for transactions.
- File of maximum 50MB.

BLUR

2.6. Market Analysis

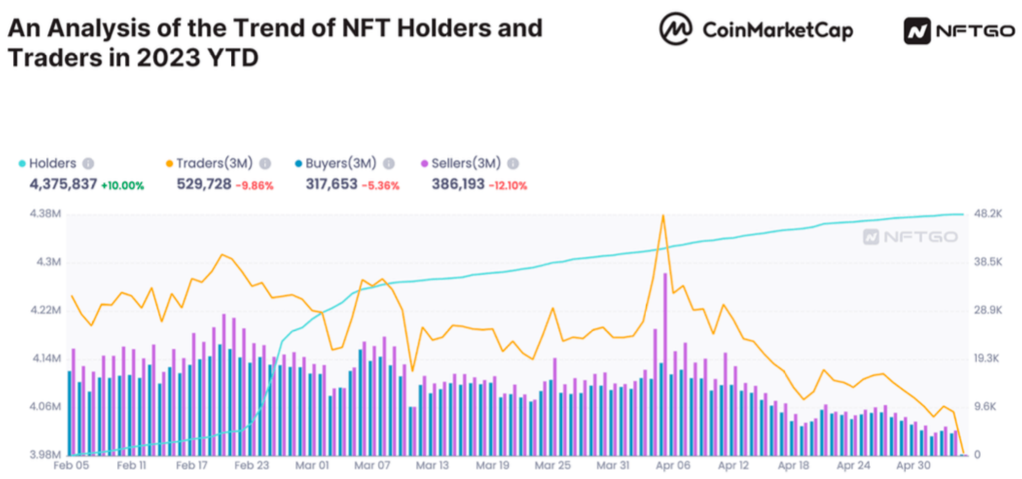
The first quarter of 2023 witnessed a substantial surge in NFT trading volume, which later experienced a downward trend. Factors such as Blur's incentives and airdrop, as well as a dispute over royalties with OpenSea (details of which will be discussed later in this document), contributed to the rise in NFT transactions. The trading volume reached its zenith on February 22nd with 74,550 ETH, before gradually declining post-March.



Fluctuations in NFT Market Capitalization and Trading Volume Throughout 2023 YTD

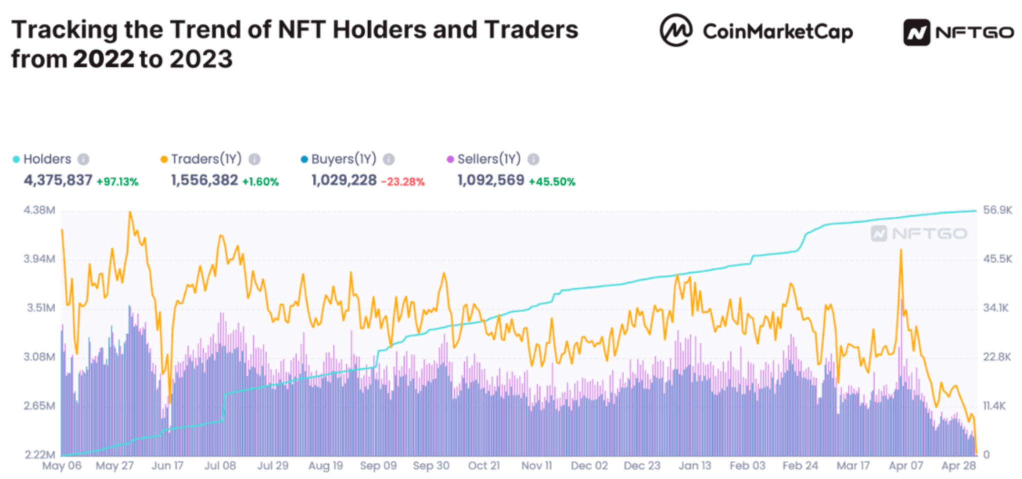
Source: NFTGo

As per the data from NFTGo, there was a notable dip in the number of NFT holders to its 12-month low on April 19th, marking a total of 11,187 traders. Despite this, the total count of holders saw an approximately 12.62% growth, amounting to roughly 4.3 million by the end of April. It is of interest to highlight the pronounced increase in the number of holders during early and late February, a trend possibly driven by the growing interest in the zero-fee ecosystems of Blur and Yuga Labs.


An Analysis of the Trend of NFT Holders and Traders in 2023 YTD

Source: NFTGo

It's significant to note that the recent downturn in NFT transactions has been concurrent with a year-long trend of a decreasing buyer-to-seller ratio, which suggests a shift in market dynamics.

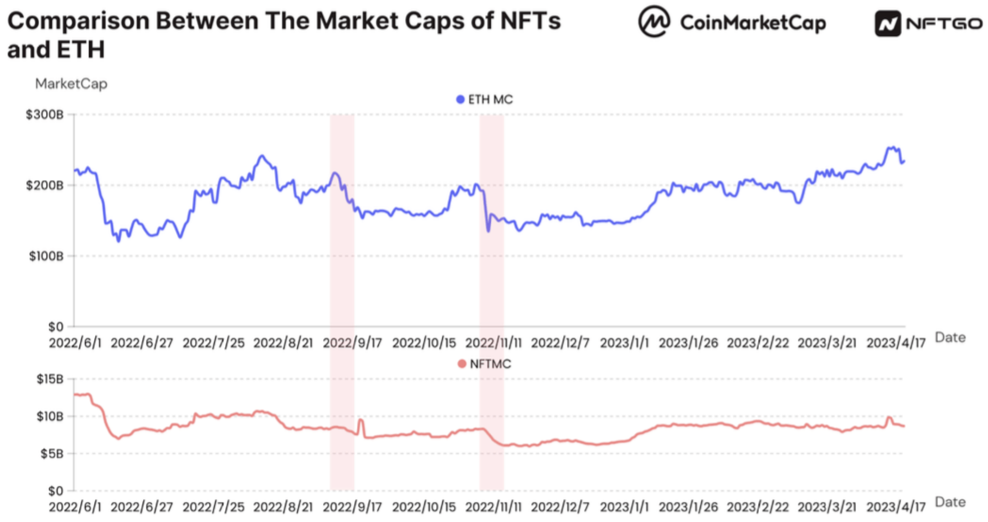

Tracking the Trend of NFT Holders and Traders from 2022 to 2023

Source: NFTGo

A significant reduction in floor price over time has been observed in numerous high-value NFT projects. For instance, the Bored Ape Yacht Club project witnessed a substantial decrease in floor price, decreasing by two-thirds from its highest point of 153.7 ETH in April 2022 to less than 50 ETH.

We are currently observing in the NFT market not a downturn but the beginning phase of its second significant cycle, which trails behind the broader crypto market. The correlation coefficient between Ethereum (ETH) and NFT markets is, on average, 0.76. This suggests that the NFT market isn't as susceptible to wild swings as the conventional cryptocurrency market. Typically, the NFT market doesn't respond instantly to severe volatility. For instance, many leading NFTs saw comparatively minor decreases in their dollar-based prices when ETH's value dropped.

The chart below exemplifies that even when the market capitalization of ETH declines, the NFT market capitalization doesn't respond immediately and maintains greater stability. The NFT market cap index has a variance of 1.35E+09, considerably smaller than the ETH market cap index's variance of 2.99E+10.

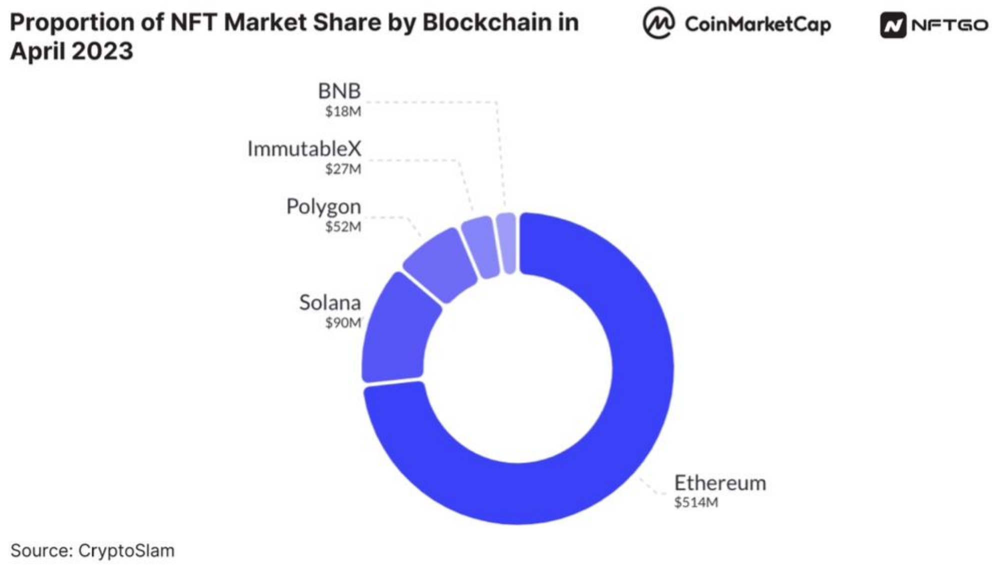


Source: CoinMarketCap, NFTGo

In the past two years, the market capitalization of NFTs and the number of NFT owners have expanded tenfold. Despite this impressive increase, the NFT market constitutes about a tenth of the entire ETH market capitalization, implying it's still a relatively small sector. However, the ongoing growth of the NFT market points towards its enormous future potential.

The period from late 2021 to early 2022 saw an extraordinary surge in the NFT market, now often referred to as the "NFT Bull Market." Yet, the market started to cool down in the latter half of 2022. As the NFT market is mainly community-driven, innovative concepts and trending topics will play a crucial role in triggering the subsequent growth wave.

As of 2023, Ethereum continues to be the dominant Layer-1 platform for the NFT market, followed by Solana, Polygon, and BNB Chain. In April 2023, the NFT trading volume on Ethereum reached $514M, accounting for nearly 70% of the global market's trading volume. Solana came next with a trading volume of $90M (12%), followed by Polygon (7%), while other platforms accounted for less than 5% of the trading volume.



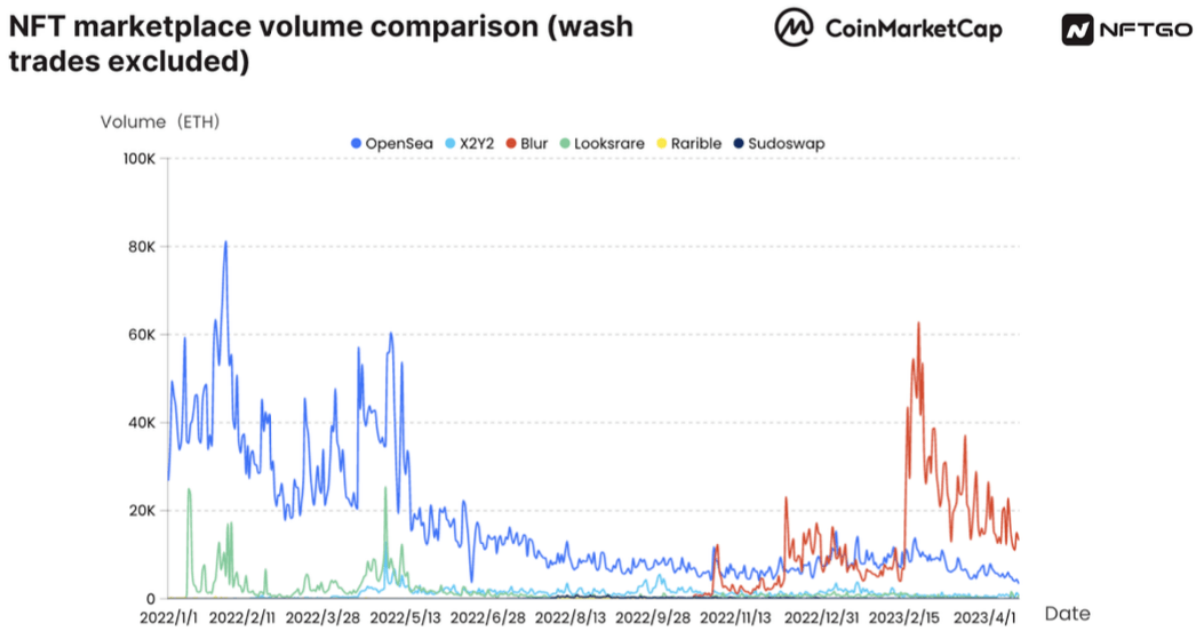
Proportion of NFT Market Share by Blockchain in April 2023

Source: CryptoSlam

Ethereum maintains its dominant position in NFT transactions, constituting over half of all transactions in 2023 to date, with a monthly transaction volume fluctuating between one to two million. Conversely, Solana's performance in the early part of 2023 has been underwhelming, a residual effect of the irregularities experienced in 2022, such as abnormal network transactions and the aftermath of FTX's insolvency. Combined with the robust competition from Ethereum, Polygon, and emerging Layer 1s like Aptos, these factors contribute to a gradual decline in Solana's trading activity.

The Current State of NFT Marketplaces

Until December 2022, OpenSea led the market in terms of trading volume. Nevertheless, with the introduction of Blur, a swift increase in trading volume was observed, allowing it to outstrip OpenSea.

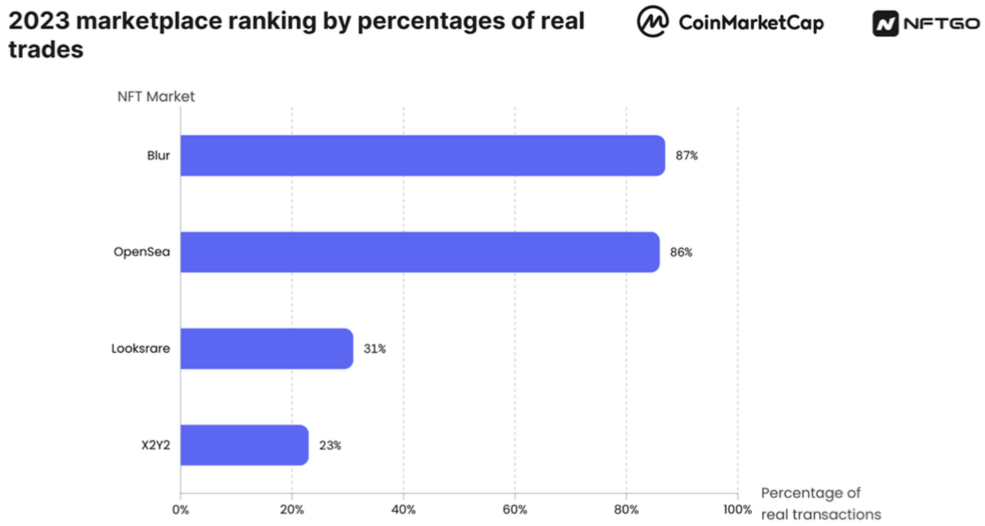


Source: NFTGo

The diagram above signifies a considerable escalation in Blur's trading volume following its airdrop on February 15th. Data gathered from January to April of the current year reveals that Blur has exceeded OpenSea's performance by 120% in cumulative trading volume. However, OpenSea possesses approximately three times the number of individual traders compared to Blur, which has close to 590,000 traders. This implies that Blur's trading community predominantly consists of professional traders who execute high-frequency trades with significant average amounts. In relation to the count of addresses, OpenSea has seen a modest growth of 12%.

Furthermore, NFTGo offers GoTrading solutions that can assist in the expedient and effortless establishment of your own NFT marketplace aggregator.

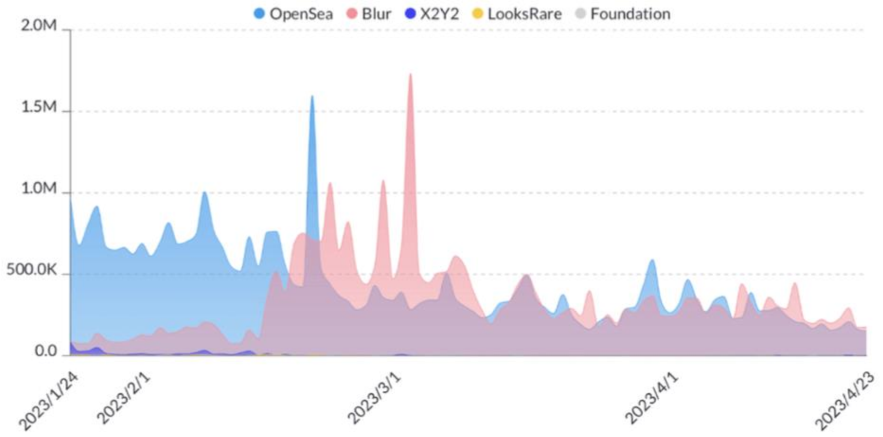
In the initial quarter of this year, Blur and OpenSea demonstrated an almost equal proportion of genuine transactions, significantly exceeding other marketplaces. Their combined influence has made a substantial impact on the current market landscape, as evidenced by data trends and their widespread social recognition.



Source: NFTGo

Based on the research by Hildobby, OpenSea had traditionally been the leader in royalty revenue. However, since mid-February, Blur has overtaken OpenSea, demonstrating an increased revenue from royalties and maintaining this status. Throughout March, Blur and OpenSea were the predominant earners of royalty revenue, but Blur achieved a maximum revenue of $1.7M on March 3rd. In contrast, OpenSea's royalty revenue declined to a minimum of $300K by the end of February after reaching a high of $1.5M on February 20th. This disparity indicates a shift in market dominance, positioning Blur as the new frontrunner in the royalty market share. The success of Blur can be attributed to the strategic introduction of optional royalty fees and zero gas fee policies, specifically appealing to the most cost-conscious users in the market.

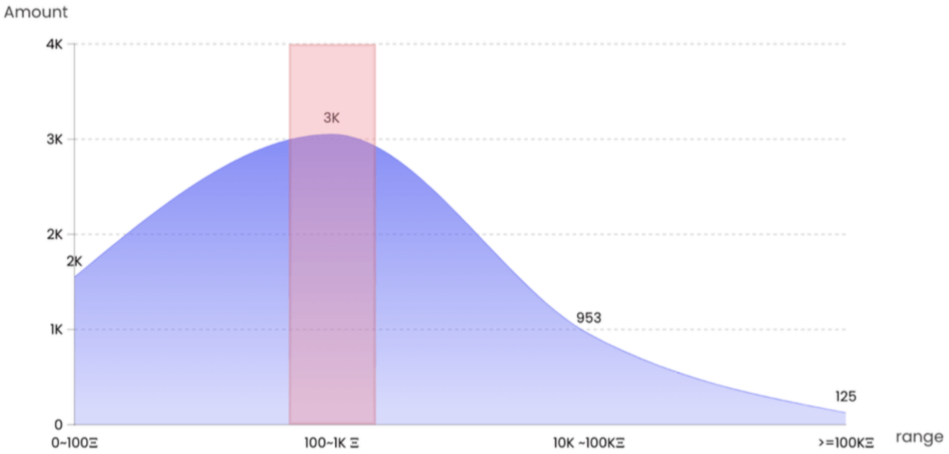
Royalty fees



Source: Dune Analytics

From mid-February onwards, there has been a significant decline in the comprehensive marketplace fee across prevalent NFT marketplaces. To compete with Blur's economical fee structure and to draw a larger user base to solidify its market standing, OpenSea introduced a temporary period of no marketplace fee along with an optional royalty. However, this strategy didn't prevent a decrease in OpenSea's total transaction volume, which plummeted from a January peak of more than $600K to a low of approximately $50K in March.

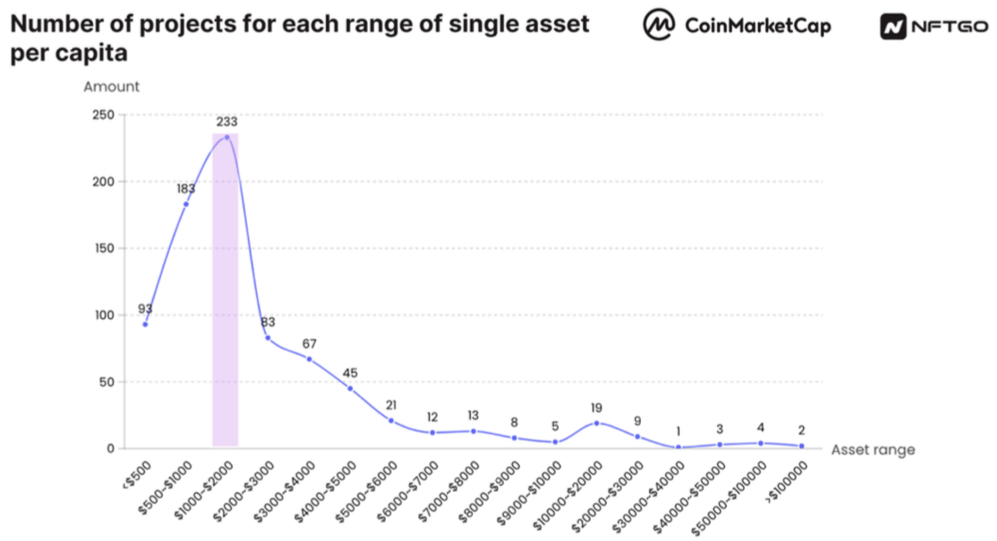
Distribution of market capitalization and price ranges for all NFT projects



Source: NFTGo

As per the data from NFTGo, over half of the NFT projects possess a market capitalization that falls between 100 and 1000 ETH, equivalent to approximately $0.2M to $2.1M as of April 2023. The next notable category represents those within the 0 to 100 ETH range, accounting for a total of 1550 projects. Remarkably, 125 projects have a market cap exceeding 100K ETH.

Upon examining the distribution of projects, it is clear that the top 50 projects make up less than 1% of the overall number of projects, but they command about 52% of the total market cap. This observation demonstrates that the distribution of NFT projects and market cap substantially outstrips the 80/20 rule, as indicated by the distribution of whales and average investors.


Number of projects for each range of single asset per capita

Source: NFTGo

2.7. New Architecture Based on Smart Contracts and Oracles for NFTs

In the context of NFT evolution, the advanced proposal aims to introduce an additional layer of security by blending the capabilities of smart contracts with the strength of oracles. Throughout the process of purchasing or "minting" an NFT, before the action can be finalized, the smart contract is activated. This contract consults an oracle, which in turn interfaces with an external API to fetch a risk value, representing the likelihood that the user in question may harbor malicious intentions. Should this risk value surpass 50%, the transaction is promptly halted, thereby shielding the average user from potential interactions with harmful entities.

Adopting such an architecture offers a range of significant advantages. Foremost, security is substantially heightened. By introducing a risk-based evaluation layer, the odds of interaction with fraudulent or malicious entities are considerably diminished. This augmented protection ensures that users can operate within a more secure and trusted exchange environment, minimizing the risks associated with digital transactions.

Furthermore, the automation brought about by the interplay between smart contracts and oracles ensures efficient transaction management. This implies there are no delays induced by the verification process: every action is executed swiftly, ensuring users do not have to wait to finalize their operations. This expedience, paired with the objectivity ensured by predefined algorithms, offers a superior user experience.

Another positive aspect revolves around the flexibility of this approach. Given that the architecture relies on external APIs, it can evolve and adapt to the shifting needs of the NFT marketplace. This means that new evaluation metrics or security criteria can be seamlessly integrated into the system, ensuring that the platform remains at the forefront and responds promptly to emerging threats or opportunities.

Lastly, the level of transparency provided is of paramount importance. Users are not only safeguarded but are also acutely aware of the protective mechanisms in place. This engenders greater trust in the system and ensures that users are informed about the verification modalities and decisions made by the platform.

However, the reliance on oracles poses a primary challenge. Being intermediaries between the blockchain and the external world, a compromised oracle could lead to erroneous decisions by the smart contract. Simultaneously, the constant querying of oracles and APIs could introduce additional costs, making transactions somewhat more expensive for users. The complexity introduced by this verification layer might also heighten maintenance and monitoring system requirements. And notably, there's the risk of false positives where legitimate users could be erroneously flagged as high-risk.

In summary, the proposal to integrate smart contracts and oracles into the NFT ecosystem seems to offer a plethora of benefits. If managed diligently and continually optimized, this architecture holds the potential to revolutionize the NFT world in terms of security and reliability.

3. Cybersecurity Problems

3.1. **Issue in Marketplace**

In this section, I pinpoint vulnerabilities inherent in the structure of NFTMs that, when exploited, lead to substantial financial threats for both the platforms and their users. To collate data for this investigation, I drew from documented security breaches, assault instances, and misuses highlighted in diverse blogs and scholarly reports, as well as firsthand engagements with specific marketplaces and their official literature. I organized the insights by linking them to later-discussed marketplace activities and aimed to numerically assess the frequency or effect of these vulnerabilities when feasible. In conclusion, I conducted a comprehensive analysis of these issues across all examined marketplaces.

3.1.1. User Authentication

Authentication of Identity.

Historically, tangible art has been implicated in money laundering activities. The emergence of NFTs could potentially simplify such illicit practices, given the anonymity of transactions and the absence of physical artwork transportation. Implementing stringent identity checks is a proactive measure against these malpractices. Renowned cryptocurrency exchanges like Coinbase and Binance US adhere to strict regulations. To register on these platforms, users must furnish detailed personal information, such as their name, address, and Social Security Number, accompanied by corroborative documents. Absent identity validation, the platform is either inaccessible or permits only limited financial transactions. Upon exploring various NFT Marketplaces by registering, it was observed that none had adopted the KYC protocols or instigated AML/CFT measures. Consequently, users can not only maintain anonymity but can also establish multiple accounts, making it challenging to associate them with a single individual.

Two-factor authentication

Incorporating Dual-Authentication Mechanisms (DAM) significantly augments the resilience of authentication systems reliant on passwords. Established financial entities, including banks, brokerages, and digital currency platforms such as Coinbase and Binance, frequently offer

DAM, but it remains inconsistently adopted across Non-Fungible Token Marketplaces (NFTMs). For instance, Sorare oversees a user's digital wallet. Consequently, a malicious actor gaining access to an account can retrieve the Ethereum private key linked to that wallet and conduct transactions on the user's behalf. While Sorare does offer DAM, it isn't activated as a default setting. For Nifty patrons, DAM remained a choice until a notorious security breach in March 2021. Preliminary evaluations indicated that none of the affected accounts had DAM in place during this breach.

3.1.2. Token Minting

Token Contract Authenticity.

A token contract achieves "authenticity" when its source code is presented on Etherscan. Given the intricate operations of these token contracts, it's simpler to assess source code rather than bytecode. Ensuring the integrity of external token contracts is paramount since they might contain errors or malevolent code. For instance, OpenSea users reported a problematic token contract that failed to transfer tokens post-purchase. Furthermore, to enhance the value of certain NFTs, some NFT initiatives assert a limited circulation quantity (emphasizing rarity) for a token. A harmful token contract can exploit this by creating tokens beyond the stipulated rarity, thereby diminishing the token's value to the detriment of purchasers. A flawed contract might expend gas without executing any substantial operation, as evidenced by the majority of Purchase events associated with the CelebrityBreeder contract, which ended in errors. In an ideal scenario, prior to minting NFTs, an NFT project would expose the source of the associated token contract to public examination to affirm its legitimacy and functionality. Regrettably, no current NFT platforms requiring external token contracts stipulate the necessity for these contracts to be open-source.

In an examination of the prevalence of closed-source NFT tokens, a review of 11,339 token contracts revealed that 8,122 (71.63%) were open-source. The remaining 3,217 (28.37%) were closed-source. Specifically, 7,850 (96.65%) of the open-source and 3,209 (99.75%) of the closed-source tokens are associated with OpenSea.

The removal or "take-down" of NFTs by NFTMs, due to reported abuses or terms and conditions violations, serves as an indirect, albeit potent, indicator of a token's malicious nature. Based on observations, OpenSea removed 1,765 (55.00%) closed-source tokens, representing a trading volume of $328.8M USD, within a specified timeframe. In comparison, only 606 (7.72%) open-source tokens were taken down in the same period.

Tampering with token metadata.

The token's metadata contains a reference to the associated asset. Therefore, if there's an alteration in the metadata, the token's relevance diminishes. The ERC-721 protocol, which underpins NFTs, does permit the amendment of a token's metadata. Yet, when an NFT embodies a specific asset, like a piece of art that has been transacted, modifying the metadata breaches the buyer's anticipation. The metadata's content and location are determined during the minting process. An unscrupulous creator or owner, referred to as 'A', can post-mint manipulate the metadata in two primary ways: by adjusting the metadata_url, and by altering the metadata's content. While interventions at the contract level may restrict, if 'A' oversees the domain, metadata located on external web domains can be easily adjusted. This latter form of manipulation can be circumvented by housing the metadata on IPFS. As the IPFS-stored object's URL incorporates its content hash, the metadata remains unmodifiable without changing the NFT's recorded URL.

Within internal token contracts, platforms like CryptoPunks, Foundation, Rarible, and Nifty do not permit alterations to the metadata_url of an NFT. Conversely, Axie grants creators the flexibility to amend the URL as needed. Meanwhile, platforms such as OpenSea, SuperRare, and Sorare permit URL modification by the creator until the initial sale is conducted. Except for Foundation, which necessitates the storage of metadata on IPFS, other NFT management systems are vulnerable to the secondary type of attack when using internal contracts. Given that no NFT management system that supports external token contracts implements safeguards against metadata interference, both attack forms remain plausible. A research endeavor assessed the metadata_urls of all 9,064,767 external OpenSea assets at equidistant intervals over half a year, specifically in June 2021, September 2021, and December 2021. It was observed that the metadata_urls for 89,089 (2.89%) and 35,446 (1.15%) assets underwent changes between the initial two and the subsequent two evaluations, respectively.

3.1.3. Token Listing

Principle of Restricted Access.

In the process of listing an NFT, the NFTM assumes command over the token to facilitate the transition of ownership from the seller to the purchaser upon completion of the sale. For this mechanism, the NFTM should either possess the NFT directly, implying the original owner transfers the asset to a holding account E during the listing phase, or act as a controller: a designated Ethereum account C endowed with the authority to oversee that particular NFT on the owner's behalf, or function as an operator: an Ethereum account O vested with the power to supervise all the NFTs within that series.

Adopting the holding model as outlined in the scenario presents vulnerabilities since a singular holding contract/wallet E, under the supervision of the NFTM, becomes the custodian for all assets transacted on the platform. Consequently, the integrity of all assets in a marketplace hinges on the safeguarding of the holding contract or the external entity governing such a contract.

The current design significantly deviates from the principle of minimal privilege. Consequently, a flaw in the contract or disclosure of the external account's private key might endanger the security of all housed NFTs. Platforms such as Nifty, Foundation, and SuperRare employ this method. A more secure strategy would involve either the second or third method, where a proxy contract, either C or O, initiated by the NFTM assumes the role of the NFT's overseer or the manager of the full NFT set. Mandated by the marketplace agreement, the NFTM is only authorized to move an NFT when it's listed for purchase and the stipulated sum is first settled with the seller. This mechanism ensures the NFT token's security even in the event of a marketplace breach. Should an NFT owner's private key be exposed, it would endanger only that specific NFT or its set, in contrast to the entirety of NFTs in the escrow structure.

Invalid caching.

When presenting an NFT for sale, platforms such as OpenSea and Rarible utilize a local caching mechanism to reduce redundant retrieval requests for the related images. A discrepancy arises if the image undergoes alteration or removal, causing the cache to become misaligned. This discrepancy may inadvertently mislead a potential purchaser into acquiring an NFT, which, due to the outdated cache, may display an asset that is either missing or altered. To gauge the implications of this caching dilemma, one can assess the percentage of image_urls that are unobtainable (resulting in a non-200 HTTP response). It was found that 32.30% of tokens were unreachable. Nevertheless, of those unreachable images, OpenSea continued to cache 2,691,030 (or 68.21%), giving the false impression that the associated NFT asset remains intact. A notable instance of this misalignment is observed in the "Gods Unchained" collection, a certified collection with a cumulative trade volume of 19.8K Ether.

Seller and collection verification.

Verified sellers or collections often receive preferential status on Non-Fungible Token Marketplaces (NFTMs) and are more prominently noticed by prospective buyers. However, the criteria for such verification are often not standardized, and the final approval often lies with the NFTMs' judgment. Typically, sellers are asked to provide social media accounts to confirm their identity, share contact details, meet a specific trading volume threshold, and sometimes even submit original files of their digital creations. While platforms like Foundation enforce strict verification for all sellers, others, such as OpenSea and Rarible, consider verification as optional. Consequently, buyers on these latter platforms need to exercise caution and due diligence, which inadvertently exposes them to heightened risks.

The monetary incentives associated with verification have led to various manipulative tactics, including:

- Badge Counterfeiting: There have been instances where fraudsters have manipulated profile images by superimposing verification badges, creating a visual semblance to legitimately verified profiles.
- Deceptive Representation: Taking advantage of lenient verification methods, deceitful entities have verified their counterfeit profiles using mere social media handles without validating the actual ownership of these accounts.
- Manipulated Transactions: OpenSea's criteria for collection verification stipulate a minimum trading volume of 100 ETH - a challenging threshold for new collections.

Consequently, this has driven individuals to engage in 'wash trading,' wherein fictive transactions occur across multiple accounts, all owned by the perpetrator, to falsely amplify sales volumes. To underscore the financial motivations driving verification misuse, one must consider the sales figures and revenue generated by both verified and non-verified sellers and collections on OpenSea. While a mere 0.40% of sellers and 0.77% of collections on OpenSea have been verified, the average sales for each verified seller and collection exceed their non-verified counterparts by factors of 10 and 1,059, respectively. Following this, an evaluation was conducted on the effectiveness of the NFTM verification processes in curtailing misuse. In an ideal scenario where the verification system is infallible, a verified collection would not possess malicious attributes and consequently, would never face removal. However, the findings show that within a span of six months, 4.88% of verified collections and 4.78% of non-verified ones were removed from OpenSea. This suggests that while verification endeavours to curtail misuse, it doesn't achieve full success in this endeavour. The removal of verified collections implies that certain malicious entities can bypass the verification protocols.

3.1.4. Token Trading

Lack of transparency.

NFTs represent asset ownership credentials that are catalogued on the blockchain, facilitating public validation. Within a decentralized framework, the sale of an NFT is orchestrated by a marketplace contract, Cm, which engages the transfer() protocol of the token contract, Ct, enabling the token's shift from seller to buyer. Each associated transaction and transfer is discernible on the blockchain. The transaction details typically encompass the current owner's address (seller), the prospective owner's address (buyer), the transactional value of the NFT, and (iv) the timestamp of the ownership transition. The ERC-721 ownerOf() protocol further simplifies the process of ascertaining current token ownership. Utilizing the sales data alongside this protocol facilitates a comprehensive reconstruction of an NFT's ownership and sales lineage.

Conversely, when sales data and transactional details are kept off-chain, verifying trades and tracing the ownership lineage of an NFT becomes unfeasible. Furthermore, unscrupulous NFT marketplaces might exploit this by concocting fictitious sales logs, artificially boosting trading activity and volume. Records stored off-chain are vulnerable to alterations, and suppressions, and could be lost if the NFT marketplace's database fails. From our research, only Nifty utilizes off-chain logs. Upon item listing, Nifty assumes responsibility for the NFT by transferring it ($T1$) to a holding wallet. While the asset remains under Nifty's guardianship, numerous transactions might transpire, yet the blockchain remains devoid of any sales log. When the owner opts to retrieve the NFT from Nifty, the platform facilitates ($T2$) its return to the owner's account. Given that only $T1$ and $T2$ are discernible on the blockchain, any intermediate ownership shifts and sales engagements remain obscured.

Fairness in bidding.

NFTMs facilitate bidding in two primary ways: on-chain, via a smart contract that mandates bid amounts to be lodged during the bidding process, or off-chain, through the NFTM dApp that upholds an order book, eliminating the need for initial payment. Off-chain mechanisms present issues of equity as they can be exploited by both the NFTM administrators and the users. Given that bids remain undisclosed on the blockchain, NFTMs have the potential to exaggerate bid volumes to generate enthusiasm. Additionally, the absence of monetary transfers makes bid placement cost-effective. This leaves such NFTMs vulnerable to 'bid pollution,' where a surge of non-committal bids is placed on assets. With no financial commitments, a significant portion of these bids often collapse due to inadequate funds in the bidder's account upon execution. In contrast, on-chain bidding incurs gas fees for bid placement/cancellation, deterring ill-intentioned parties from initiating false bids, thus minimizing manipulative behaviours. Furthermore, on-chain procedures necessitate upfront bid amount reservations, ensuring their consistent success upon settlement. In platforms like OpenSea, we've noted seller grievances stemming from unsuccessful (attempted) sales, often because the WETH reserves of the top bidders fall short of their proposed amounts.

Royalty distribution and marketplace fee evasion.
Should a royalty be established, each transaction should yield a fee benefitting the creator. However, our research has identified potential loopholes in the royalty frameworks:

- Inter-platform discrepancies. As outlined in Section 3, royalties are facilitated either by the marketplace contract or the dApp, each specific to a given NFTM. Moreover, NFTMs do not exchange royalty data amongst themselves. Consequently, a royalty specified on one platform may not be recognized on another. Exploiting this disparity, a malevolent seller might circumvent royalty payments by conducting transactions on a platform where the royalty hasn't been defined, even if it's established on another platform.

- Lack of enforced compliance. Neither royalties nor marketplace charges are obligatory in ERC-721 token contracts. This loophole enables a malevolent seller to bypass both by directly transferring (through ERC-721 transfer()) the NFT to a purchaser and finalizing the payment outside the platform. Both the royalty and fees could be incorporated within the transfer function of the token contract, though the added complexity could inflate the API costs.

- Post-sale adjustments. Platforms like OpenSea and Rarible grant creators the flexibility to alter the royalty percentage subsequent to the initial sale. At present, the royalty is derived from the seller's listed price. In a conceivable exploitative scenario, a creator might entice a buyer, let's call them Buyer B, by stipulating a minimal royalty, only to augment it after the primary sale. During subsequent sales, Buyer B might remain oblivious to this amendment, resulting in a higher-than-expected royalty payment to the creator.

The potential abuses of unconditional token transfer to evade NFTM fees and royalties. The question of evasion appears when a seller S lists an NFT on a marketplace to gain popularity, but executes the trade off-platform, entirely bypassing the marketplace protocol. There could be two possible cases. Seller S might trust the buyer B and, therefore, transfer the NFT first. After that, B settles the payment. In the other case, the order is reversed.

3.2. **Fraudulent user behaviour**

3.2.1. Layer-8 Risk

At present, the traditional OSI model of computer networks doesn't include a Layer-8. Nevertheless, a group of astute engineers humorously introduced the term to represent elements associated with the user not encompassed by the standard seven layers of the OSI model. In this context, we will refer to "Layer-8 risks" to denote user-related discrepancies that fall outside the conventional framework.

Historically, it's believed that a minuscule proportion of security protocols mentioned the importance of enlightening and instructing users and individuals intrinsic to systems and operations.

Consequently, it is evident that traditional software development lifecycle processes (SDLC) inadvertently introduce numerous unanticipated vulnerabilities, potentially jeopardizing end-users and leading to considerable detriment and loss.

Moreover, contemporary threats and malicious entities differ substantially from those experienced in the late 1990s and early 2000s. Modern attackers emulate tactics analogous to a human opponent in combat, conducting detailed reconnaissance on their targets, and selecting specific techniques, tools, and engagement procedures tailored to individual victims. The MITRE ATT&CK framework is a widely acknowledged reference, enumerating over 20 techniques that contemporary attackers employ before initiating a breach. The 2021 report on Data Breaches by Verizon emphasizes that a substantial portion of breaches originate from phishing ventures or usurped credentials, indicating a decline in malware as an initial entry technique. Nonetheless, malware remains an instrument of choice post-initial penetration into the target system.

The potential for security risks associated with users, often termed as Layer-8 vulnerabilities, poses a significant challenge for the Web3 and decentralization trajectory, particularly for NFT platforms such as OpenSea.

3.2.2. Inadvertent or User Error Risks

Cryptocurrency technology is often critiqued for its intricate nature, which can contribute to an increased frequency of user mistakes. Such errors can pose threats to one's finances, reputation, or personal privacy. A significant concern related to Ethereum is the considerable transactional costs, termed as "gas fees." Each transaction within Ethereum incurs these fees, which can be exorbitant, prompting some to argue that Ethereum predominantly caters to affluent individuals or early cryptocurrency adopters. In the realm of NFT trading, there have been documented instances where users inadvertently err in their transactions in their pursuit to circumvent these gas fees.

3.2.3. Phishing risk

Phishing endeavors are prevalent strategies employed by nefarious entities in the digital domain. These stratagems often utilize automation, targeting a broad user base to achieve maximum gains with minimal exertion. This approach is especially favored given that prominent NFT enthusiasts and facilitators are conspicuous, rendering them susceptible. An illustrative instance of such a breach was encountered by NFT aficionado Todd Kramer, who was divested of 16 NFTs spanning three collections, inclusive of eight Bored Ape NFTs, cumulatively valued at approximately $1.7 million. While OpenSea intervened to immobilize the pilfered assets, such incidents underscore the ambiguities related to affirming genuine NFT ownership and highlight the inherent limitations of centralized architectures in the realm of web3 and decentralized holdings.

In June 2021, the NFT artist known as Fvckrender revealed that he was deceived into accessing a malware-infested file sent to his social media profile. This action permitted an unauthorized user to infiltrate his digital financial repositories. Subsequently, the intruder reportedly expropriated 40,000 Axie Infinity tokens, approximating a value of US$4 million. Likewise, in December 2021, an art curator and NFT enthusiast disclosed a loss of 16 NFT tokens due to a phishing scheme. The pilfered NFTs, stored in the curator's active digital wallet, had an estimated worth of around US$2.2 million.

3.2.4. Counterfeit NFT Creation

The legitimacy of an NFT is confirmed by the smart contract overseeing the assemblage. To guarantee the authenticity of a token being purchased, prospective buyers should cross-check the contract address of the assemblage with trusted sources, such as the project's official website, prior to finalizing the acquisition. Regrettably, many purchasers are uninformed about potential forgeries or the methods to authenticate an NFT. They often base their judgments solely on the titles and visual representations in the marketplaces, paving the way for malevolent entities to introduce deceptive NFTs. Our observations revealed counterfeit methods such as:

Utilizing analogous collection titles. Some deceptive NFTs adopt titles of collections or individual items that echo the genuine ones. A prevalent tactic involves replacing ASCII characters in the authentic title with visually similar non-ASCII characters. To counteract this misuse, OpenSea imposes limitations on using renowned collection titles and specific unique characters. Nevertheless, shrewd individuals often find ways to evade these restrictions, perhaps by appending a period (.) to a title or interchanging an upper-case letter with its lower-case counterpart, as seen with a forged version of the "CryptoSpells" collection termed "Cryptospells." Furthermore, such restrictions may inadvertently inconvenience genuine users. For instance, French participants expressed discontent regarding the prohibition of accented characters in their collections.

Duplicate image URLs: Certain counterfeit NFTs link to pre-existing assets, effectively replicating the image URLs of authentic NFTs. Take, for instance, the renowned CryptoPunks collection. Technically, a deceitful individual could initiate her proprietary token contract on the blockchain and generate tokens associated with CryptoPunks. A potential purchaser, focusing solely on the visual elements of a collection, may be misled by the CryptoPunks visuals, potentially confusing the counterfeit NFTs for genuine ones.

(iii) Analogous visuals: Rather than replicating the image URL, an unscrupulous actor might duplicate the digital asset and then create an NFT linked to this duplicate. Currently, no NFTM has implemented similarity checks to determine if a media file has previously been associated with other NFTs.

3.2.5. Trading Malpractices

In a detailed study on illicit trading activities, the focus was predominantly on unsanctioned practices like wash trading, shill bidding, and bid shielding. The researchers emphasized the significance of these behaviors in the context of NFTMs and made strides in constructing heuristic models geared towards spotting such malicious activities. This study sifted through an extensive dataset comprising 13,628,411 assets and 354,535,763 events. The main objective was to quantify the scale and implications of these deceptive operations across the prominent seven NFTMs.

Regarding their approach to data modeling, the study tapped into event information coupled with Ether transaction records. This facilitated the extraction of specific NFT-related actions, including but not limited to transfers, sales, and bids. Through this process, they curated four specialized relational graphs, each serving a distinct purpose: a sales-centric graph (Gs), a bidding graph (Gb), a payment-focused graph (Gp), and an asset transfer graph (Gt). The Gb graph was particularly noteworthy because of its intricacies, having both user and asset nodes, and directional edges connecting them, enriched with property details. Conversely, the Gs, Gp, and Gt graphs were more streamlined, predominantly featuring user nodes and specific directed edges between them.

The wash trading is highlighted as a particularly deceitful tactic. This method involves both the purchaser and the seller conspiring to falsely amplify an asset's trading volume via insincere trades. Within the NFTM sphere, wash trading is frequently employed by users attempting to simulate an exaggerated demand for a particular digital asset or creator. Another incentive behind this strategy might be the ambition to boost certain financial metrics, such as achieving verification for a specific profile or asset, or securing monetary rewards. An illustrative case in point is the Rarible platform, where users are encouraged with $RARI governance tokens; the greater their expenditure, the more tokens they're awarded. The study further suggests that numerous high-stake NFT transactions, especially those associated with renowned initiatives like CryptoKitties and Decentraland, might be tainted by wash trading.

There were findings of 9,393 instances of wash trading. This resulted in an astounding trading volume of $96,858,093 USD. This activity spanned 5,297 collections and involved 17,821 users across various NFTMs. Notably, Axie, Foundation, and CryptoPunks were the exceptions, where such practices weren't detected. The same study pointed out that from the 238,180 collections they analyzed, merely 8,869 collections boasted over $2K in trading volume. Alarmingly, 2,569 collections, which equate to 28.97%, displayed indications of wash trading.

The researchers introduced a term, 'wash_trade_factor' (WTF), to describe the proportion of a collection's trading volume that results from wash trading. If the WTF value equaled 1, it meant the entire trading was attributed to wash trades. Their data visualization in one of their figures highlighted the distribution of this factor for collections where wash trading was observed. The research notes that 1,824 collections (or 34.43%) witnessed less than 5% of their trades from wash trading. However, a concerning 1,571 collections, or 29.66%, appeared to be heavily exploited, with more than 95% of all trades being wash trades. This accounted for a significant $3,407,284 USD in trading volume.

A subsequent figure in the study delineated the relative wash trade volumes across different NFTMs. It was enlightening to note the near parity in wash trade volumes found in Rarible (49.30%) and OpenSea (50.43%). However, when considering that OpenSea's overall trading volume is 21 times that of Rarible, it implies a much higher frequency of wash trading on Rarible. This observation is further affirmed by chatter observed on Rarible's Discord platform, hinting at a rich history of wash trading episodes, particularly as malicious actors vied for $RARI tokens.

Shill bidding is a type of auction malpractice wherein the asset's final price is artificially elevated. This is achieved either by the seller bidding on their own items or through a collaborative effort with other bidders to place a series of deceptive and escalating bids. Such tactics can result in genuine bidders shouldering higher costs than they might have in a fair scenario. With the surge in high-value bids, there's a growing suspicion that a significant number of sales are tainted by this form of price manipulation.

An investigation identified 703 cases of shill bidding spread across 282 unique collections, engaging 1,211 users. Notably, Axie and CryptoPunks remained exempt from these findings. To quantify the gains from such activities, we introduced the term 'shill_profit' – essentially the added profit sellers secure through shill bidding. To break it down, if a genuine bid is placed first, followed by shill bids that elevate the price, the difference between the final shill-inflated price and the last genuine bid represents the 'shill_profit'. Indicates that unscrupulous sellers amassed a combined profit nearing $13,014,662 USD via shill bidding.

A breakdown of our findings reveals that the majority of collections, 197 to be exact, recorded only a single instance of shill bidding. Meanwhile, almost all collections registered under 20 such bids. An exception to this trend is the official collection of Foundation, which has been notably plagued by shill bidding, with 212 instances, making up 30.16% of the entire detection pool. This collection topped the charts for shill bidding. Other collections with notable shill bidding activities include SuperRare and CryptoVoxels. The latter, an OpenSea-verified collection, boasts 5.8K items and has transacted 19.2K ETH in volume.

In a notable study on auction dynamics, shill bidding was brought to the forefront as a recurrent auction fraud. This deceptive practice involves sellers artificially raising the final asset price, either by placing bids on their own items or by collaborating with other bidders to place increasingly substantial false bids. Such a tactic can cause sincere bidders to pay more than they otherwise might have. Given the surge in high-value bids on assets, there's a growing suspicion that a significant number of sales are tainted by this artificial price escalation. The researchers identified 703 shill bidding incidents spanning 282 collections with the involvement of 1,211 users. Interestingly, all NFTMs showed evidence of this activity, except for Axie and CryptoPunks.

To gauge the economic impact, the study introduced the 'shill_profit' metric, which represents the gains accrued by sellers due to shill bidding. If legitimate bids are placed on an item first and subsequent shill bidding amplifies the price, the difference between the artificially inflated final sale price (bs) and the last genuine bid (bl) is deemed as the shill_profit. The findings were alarming: sellers raked in an aggregate profit of $13,014,662 USD from the detected shill bidding activities.

The study further delved into the frequency of these incidents across collections where shill bidding was observed. A majority of the collections (197 out of the total) had only a single shill bidding incident. However, almost all collections (281 to be exact) reported fewer than 20 such bids. The official collection of 'Foundation' stood out as a glaring outlier, being heavily tainted by shill bidding. A staggering 212 instances (accounting for 30.16% of all detected incidents) were found within this collection alone, making it the most affected of any individual collection. Other noteworthy collections, such as 'SuperRare' and 'CryptoVoxels', were also flagged for frequent shill bidding, with the latter being an OpenSea-verified collection boasting 5.8K items and an impressive cumulative trading volume of 19.2K ETH.

A study delved into the illicit practice known as bid shielding. In this malpractice, a rogue bidder, referred to as $u2$ in the study, strategically places a high bid to deter genuine bidders after a potentially colluding bidder, known as $u1$, has made a low bid. This rogue bidder then withdraws their bid just before the auction's conclusion, thereby exposing the low bid made by $u1$, enabling her to secure the auction victory. The researchers identified a total of 316 occurrences of bid shielding in OpenSea alone, spread across 117 collections and involving

471 users. Their findings suggest that such instances were mostly isolated to OpenSea due to the stricter bidding policies implemented by other NFTMs, as elaborated in their third section. Such policies include the likes of on-chain bids and the removal of prior bids when they are surpassed.

To quantify the financial implications of bid shielding, the study introduced a metric termed 'shielded_bid_difference', which calculates the gap between the bids of the two suspected colluding parties. Astonishingly, while the smallest discrepancy amounted to $200.77 USD, the largest soared to a staggering $152,606.31 USD, observed in a token from the verified Mirandus Vaults collection. The combined value of shielded bids across all 316 instances reached nearly a million dollars, summing up to $942,061 USD. The study further showcased the prevalence of bid shielding across various collections, revealing that a vast majority (113 out of 117 collections) experienced fewer than ten such instances. However, the Ethereum Name Service (ENS) topped this list with a worrying 49 instances. Interestingly, the CryptoVoxels collection also merited attention. The study corroborated complaints made by the collection's patrons on Discord, noting that a total of $24,519.27 USD was shielded in 35 instances of bid shielding. What's more, the research underscored that bid shielding isn't exclusive to less reputable collections. A significant 66.67% (or 78 out of 117) of the affected collections had been verified.

Digital Limitation Principle. The concept of digital limitation [14] refers to the deliberate constraint placed on a digital asset's abundance, typically facilitated through software protocols. An asset's intrinsic value diminishes as its ubiquity grows. NFTs, anchored by smart contracts, allow for these constraints to ensure an asset's rarity. This can be achieved under the conditions: the distinctive rarity parameter is integrated on-chain, and the contract draws upon this parameter to preclude excessive minting.

In contemporary scenarios, most items purporting to be of limited edition or rarity rely more on verbal affirmation rather than contractual assurance. Indeed, instances have been identified where items, under the guise of being limited edition, were minted beyond their declared limit. For instance, CryptoMotors, a collection accredited by OpenSea, alleges that only 150 GEN1 cars are in circulation. However, the parameter defining its rarity (GEN) is externalized, located off-chain within JSON metadata, rendering contractual enforcement of rarity unfeasible. Furthermore, the overarching Supply parameter, which dictates the total issuance of a token, remains mutable, thus allowing for potentially infinite minting.

Fraudulent Giveaways: Some NFT initiatives offer free tokens as a promotional strategy, asking participants to promote a new collection on various social platforms. However, under the guise of these promotions, swindlers often entice participants with promises of complimentary NFTs, only to levy ostensibly minor charges meant to cover gas expenses. Contrarily, these charges are frequently significantly higher than actual gas costs. Certain NFT platforms employ specific tokens as their standard currency, such as NFT-Art.Finance, which operates using the $NFTART token. There have been deceitful activities where con artists feign a sale involving either the NFT or the platform token. Unwitting users, lured by this, transfer money to specified accounts but never receive the promised NFT or tokens. Notably, authentic giveaway events have been exploited by these scammers, who imitate winners using counterfeit social media profiles, thereby redirecting the prize to their accounts and depriving the genuine winner.

4. Proposed Solution

4.1. Implementation of a Risk-Based Smart Contract

In response to the burgeoning concerns surrounding fraud and malicious activities within the Non-Fungible Token (NFT) marketplace, this chapter introduces a novel solution centered around the implementation of a blockchain-based smart contract. The core objective of this solution is to mitigate the risk of fraudulent transactions and enhance the overall security and integrity of NFT exchanges. To achieve this, the proposed smart contract leverages a sophisticated Risk Score mechanism, calculated by Anchain.AI's advanced Artificial Intelligence (AI), and integrates seamlessly with the decentralized nature of blockchain technology.

Risk Score and its Significance

The Risk Score, in the context of this solution, serves as a pivotal metric for assessing the trustworthiness of an address or entity participating in NFT transactions within the ecosystem. It is imperative to clarify that the Risk Score is specific to each blockchain address and is meticulously calculated by Anchain.AI's AI engine. The calculation process is grounded in an intricate analysis of the historical transactional behavior associated with a given address. The AI examines a wide array of parameters, including transaction frequency, patterns, transaction partners, and other contextual elements to arrive at a comprehensive Risk Score. Essentially, the higher the Risk Score, the greater the likelihood that the associated address has engaged in suspicious or fraudulent activities.

Leveraging the Chainlink Oracle for Real-time Risk Assessment

To ensure the real-time accuracy and security of Risk Score evaluations, this smart contract relies on the Chainlink Oracle. This critical integration safeguards the transactional ecosystem when interacting with external data sources, an essential consideration within the broader Web3 ecosystem. By connecting to the Chainlink Oracle, this smart contract establishes a secure channel for requesting and receiving Risk Scores from Anchain.AI's servers. The Chainlink Oracle, renowned for its decentralized and tamper-proof data retrieval capabilities, guarantees the reliability and trustworthiness of the Risk Scores, thereby bolstering the overall effectiveness of this solution.

Implementation on the Goerli Test Network

The Goerli test network serves as a strategic platform for the initial deployment of this risk-based smart contract solution. Designed to mirror the dynamics of live blockchains without the associated implications of real-world consequences, Goerli offers an environment conducive to rigorous testing. This choice facilitates iterative development, enabling adjustments and refinements based on observed behaviors, transactional patterns, and potential edge cases.

Preliminary results gleaned from this integration into the Goerli network underscore the robustness of the proposed smart contract. Furthermore, these findings suggest promising adaptability and scalability factors, both crucial for future deployment within expansive and multifaceted ecosystems.

4.2. Technical Architecture of the Decision-Making System for NFTs

The proposed architecture is articulated through a sequence of precise interactions among advanced software components and protocols, each playing a pivotal role in the management of NFT transactions. The following section delineates the specifics of each step in the process.

Frontend (React): Users, through a frontend interface developed in React, trigger a request based on standard HTTP/HTTPS protocols. This request encapsulates user metadata, NFT details, and other pertinent information.

NFT Marketplace Backend: Upon receiving the request from the frontend, the backend processes the provided data and employs the specific APIs of the Goerli testnet to forward the request to the blockchain.

Blockchain (Goerli Testnet): The request is integrated into the Goerli testnet's transaction pool, awaiting processing by validating nodes. These nodes, through consensus mechanisms, activate the designated smart contract.

Smart Contract (Solidity): The smart contract, penned in Solidity, commences its set operations. It extracts the address for verification, essentially the issuer of the request, and invokes the Chainlink oracle to procure risk-related data.

Oracle (Chainlink): Chainlink, specialized in delivering off-chain data to blockchains, upon being called by the smart contract, queries a specific API endpoint to ascertain the risk value associated with the given address.

External API and Machine Learning: This interface, rooted in a machine learning service, processes the incoming request. It analyzes the data, computes the risk, and subsequently responds to the oracle with a JSON file encapsulating the calculated risk value.

Oracle's Response: Chainlink, upon receipt of the JSON file, extracts the risk value and formats it into a blockchain-compatible structure. It then responds to the smart contract, populating a specified contract variable with the retrieved value.

Smart Contract's Decision: Leveraging the risk value supplied by the oracle, the smart contract executes its conditional functions. If the value surpasses a pre-defined threshold, the transaction is halted; otherwise, it proceeds to finalization.

The backend of the Marketplace's Response: Having received the decision from the Goerli testnet, the marketplace's backend updates its internal systems. Through advanced logging mechanisms, it tracks the transaction and formulates a response for dispatch to the frontend.

Frontend (React) Response: The frontend platform, crafted in React, obtains the backend's response, processes it, and presents it to the user, informing them of the final status of their request. In the event of an error, an additional check on the risk value of the address is also conducted here.

The meticulous design of this flow ensures significant robustness and security in the verification process, delivering a resilient and trustworthy architecture for NFT transactions.

4.3. Implementation

The intricate nuances of blockchain-based solutions, particularly within the sphere of the NFT marketplace, demand not just theoretical rigour but also a granular understanding of practical implementation. This section is poised to provide just that, elucidating the backend architecture of the marketplace underpinned by a smart contract. In aiming for a comprehensive discourse, we shall delve deep into the minutiae of the codebase, offering a guided walkthrough that demystifies each component and the interplay between them. Furthermore, a notable facet of this implementation is the incorporation of an external API call designed to fetch a risk score, an indispensable element to fortify the transactional integrity of this system.

As we traverse this section, readers are encouraged to view the code not merely as a set of instructions but as a manifestation of the conceptual foundations discussed in preceding chapters. By doing so, one can appreciate the synergy between the theoretical constructs and their tangible applications in a real-world setting. Let us embark on this journey, step by step, illuminating the blueprint of this blockchain solution.

4.3.1. Setup the enviroment

Register for an Alchemy account and initiate a new application.

Subsequently, establish a new application and generate API keys via the application dashboard. Although the Goerli testnet is an option, the Ethereum Foundation has indicated its forthcoming obsolescence.

It's thus advisable to utilize the Sepolia testnet since Alchemy offers comprehensive Sepolia support, along with a complimentary Sepolia faucet.

Configure your MetaMask for the Goerli test network integration.

Should you lack an address within the Goerli network, ensure that your MetaMask is linked to the Goerli system. Subsequently, employ a Goerli faucet to acquire Goerli ETH. This ETH is essential for the deployment of smart contracts and the introduction of NFTs to your designated marketplace.

Set up the repository

For convenience, the foundational code has been made available in the following GitHub repository. While the frontend is fully developed, it lacks a smart contract and any frontend integrations.

(github.comGitHub - alchemyplatform/RTW3-Week7-NFT-Marketplace: Road to Web3 Week7 tutorial on building an NFT Marketplace from Scratch)

Install and Start npm

Configure your environmental variables and adjust the Hardhat settings.

In the main directory of your project, which is directly within the NFT-Marketplace folder, initiate a new .env file. Then, add:

- The Alchemy API URL that was established earlier.
- The private key associated with the MetaMask wallet designated for developmental purposes.

Use Piñata to upload data to IPFS

Should you not already possess a Piñata account, it is advisable to register for a complimentary Piñata account. Subsequently, proceed to generate a Piñata API key. The steps for the said generation are as follows:

- Direct the browser to https://pinata.cloud/keys.
- Opt for the "New Key" option at the upper portion of the page.
- Ensure the activation of the Admin widget.
- Allocate a distinct name to the key.

Upon completion, a window will emerge displaying the API details. It is recommended to securely store this information for future reference.

4.4. Understand the requirements

Prior to delving into the coding aspect, it's imperative that we analyze individual pages to comprehend the required features from both a user interface and a smart contract standpoint.

List NFT page

For artists or creators, this section allows them to catalogue their NFT for marketplace consideration.

This requires input of the subsequent NFT characteristics:

- Title of the NFT
- Detailed Explanation
- Valuation (in terms of ETH)
- Visual Representation of the NFT

Upon fulfilment, this information is then integrated into the NFT marketplace.

To make this happen on the backend, we need a function called generateToken(). That takes as a parameter a URL from IPFS containing metadata of the designated price for the NFT and has the following functionality:

- Allocates a unique `_tokenId` to the specified NFT
- Stores associated data within the marketplace contract
- Upon completion, triggers a "Successful Listing" event.

The user interface performs instead the following tasks:

- Receives pertinent information related to the NFT.

- Transmits the NFT image to the InterPlanetary File System (IPFS).
- Dispatches the NFT metadata, inclusive of the image link, to the IPFS.
- Forwards the IPFS link and associated price to the createToken() procedure within the smart contract.
- Informs the user upon successful data submission.

Marketplace home page

This is the home page of the marketplace where all NFTs are listed.

To make this happen, we need on the backend side a function called getAllNFTs() that provides in output the list of all NFTs currently on sale in the marketplace.

The user interface facilitates the following capabilities:

- Retrieve all NFTs currently available for purchase by employing the getAllNFTs() method embedded within the smart contract.
- Present these NFTs in a structured grid layout.
- Allow users to select a specific NFT, thereby accessing a detailed view of its attributes.

User profile page

The profile present in the NFT marketplace delineates:

- The wallet address associated with the user.
- Information related to the NFTs held by the user.
- A systematic grid representation of the NFTs, elucidating their details.

To actualize this, the prerequisites for the backend are, a function named getMyNFTs() which yields a history of NFTs transacted by the user.

The user interface performs instaed the following task:

- Retrieve information utilizing the getMyNFTs() function from the intelligent contract.
- Examine the data to procure cumulative figures and statistical analysis.

Individual NFT Page

When selecting any NFT on the marketplace interface or via the user profile page, viewers are directed to this specific interface. This interface showcases:

- The associated metadata of the NFT.
- An option titled "Purchase this NFT" which facilitates the buying process for another user.

To realize this, the following few functions are required :

- A function designated as 'tokenURI' retrieves the associated tokenURI for a given tokenId, after which the pertinent metadata for the said tokenURI is obtained.
- The 'executeSale()' function assists in performing essential verifications and transitions the ownership when a user selects the option to "Buy this NFT".

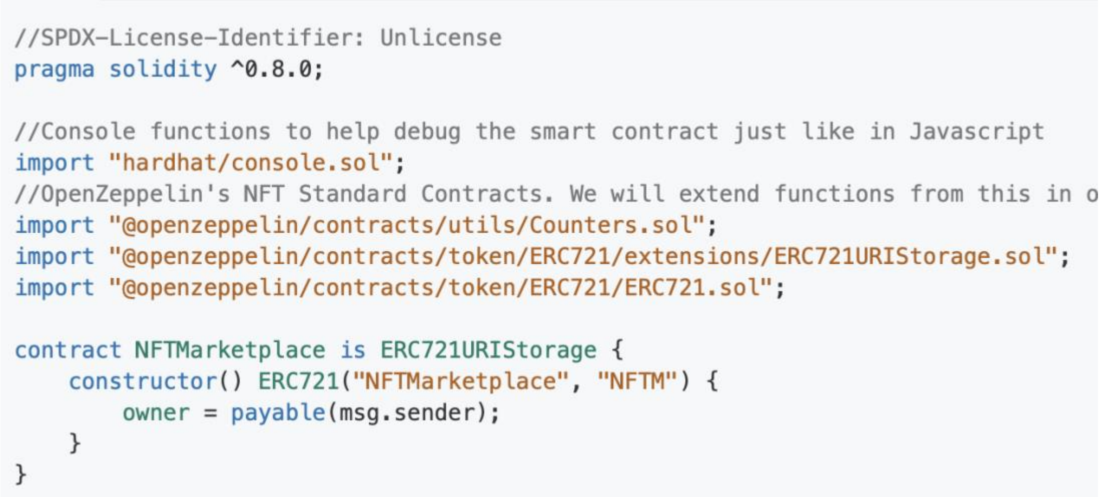
The user interface performs instaed the following tasks that does the below:

- Retrieve the tokenURI utilizing the tokenURI methodology.
- Extract data from the specified IPFS tokenURI employing the Axios protocol.
- Present the acquired data.
- Upon selecting the "Buy this NFT" option, invoke the executeSale() function.

4.5. **Smart Contract commentary**

In this subchapter, we dissect the architecture of the smart contract, elucidating the functions, state variables, and events that form its backbone. Each code snippet is complemented by an explanatory commentary, ensuring that the reader can not only replicate its functionality but also comprehend the rationale behind design choices. From the initial deployment phase to the invocation of the external API for risk assessment, we will guide the reader through the labyrinthine pathways of the contract, shedding light on its multifaceted operations. By the end of this discourse, the reader should have an intimate understanding of the contract's dynamics, poised to appreciate its pivotal role in enhancing the security and transparency of this marketplace.

NFTMarketplace.sol



```
//SPDX-License-Identifier: Unlicense
pragma solidity ^0.8.0;

//Console functions to help debug the smart contract just like in Javascript
import "hardhat/console.sol";
//OpenZeppelin's NFT Standard Contracts. We will extend functions from this in o
import "@openzeppelin/contracts/utils/Counters.sol";
import "@openzeppelin/contracts/token/ERC721/extensions/ERC721URIStorage.sol";
import "@openzeppelin/contracts/token/ERC721/ERC721.sol";

contract NFTMarketplace is ERC721URIStorage {
    constructor() ERC721("NFTMarketplace", "NFTM") {
        owner = payable(msg.sender);
    }
}
```

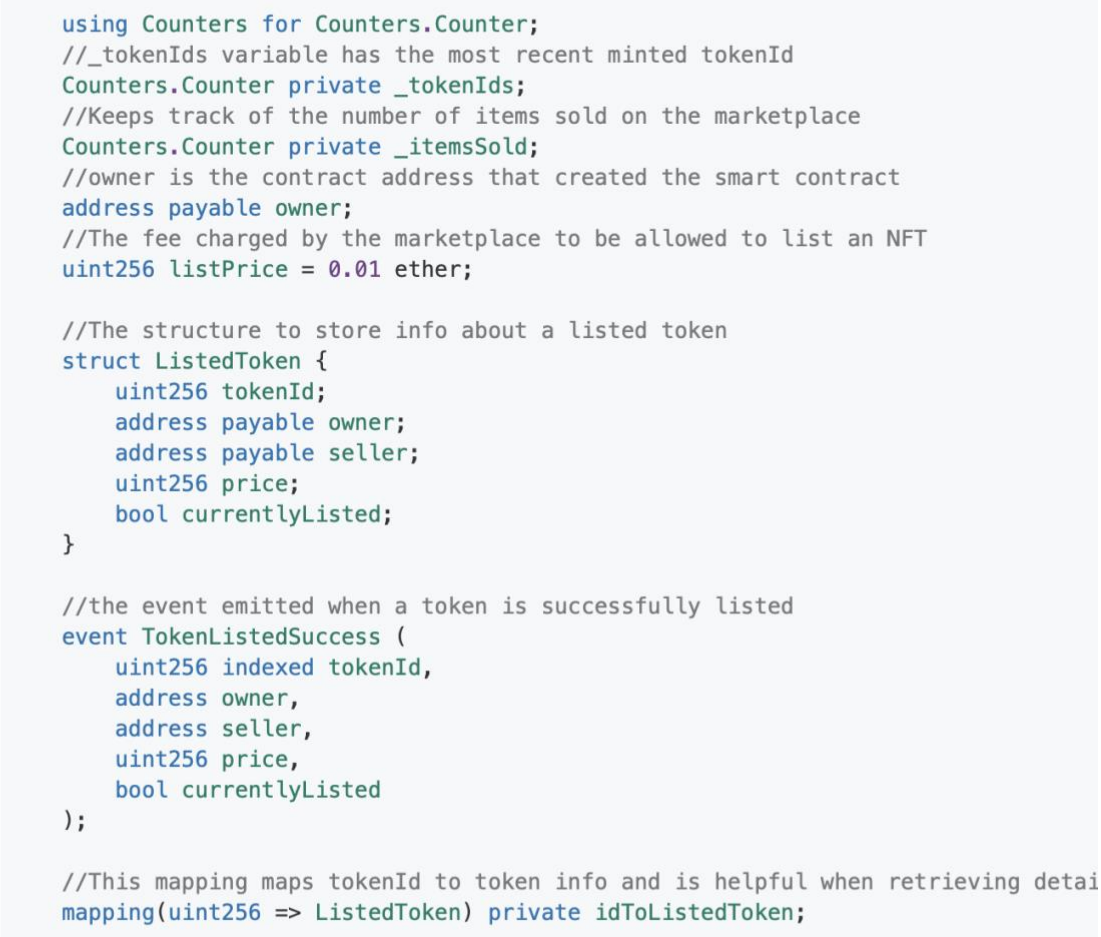
In the provided code segment, the foundation of an NFT marketplace utilizing the Ethereum blockchain is established. This foundation leans on the ERC-721 standard, which is the widely accepted specification for Non-Fungible Tokens (NFTs) on the Ethereum platform. The ERC-721 standard ensures the token's non-fungibility, a characteristic that grants each token a distinct and unique identity, ensuring its indivisibility and non-interchangeability.

The use of OpenZeppelin libraries in this codebase deserves particular attention. OpenZeppelin has positioned itself as a trusted entity in the decentralized application development ecosystem, providing a suite of tested and community-reviewed smart contract modules. Incorporating such libraries aids in mitigating security risks, thus ensuring that the foundational layers of the NFT marketplace are stable and reliable.

Specifically, the ERC721URIStorage extension from OpenZeppelin facilitates the association of each NFT with a Uniform Resource Identifier (URI). This URI typically points to a metadata JSON file that describes the NFT's attributes, such as its name, image, and any other relevant characteristics.

The constructor of the NFTMarketplace contract initializes the NFT contract with its designated name and symbol. Moreover, it immediately assigns the contract's ownership to the account deploying the contract, establishing a clear line of control.

As this segment primarily focuses on laying the groundwork for the NFT marketplace, further development is anticipated to introduce marketplace features such as listing, purchasing, and transferring NFTs.



```
    using Counters for Counters.Counter;
    //_tokenIds variable has the most recent minted tokenId
    Counters.Counter private _tokenIds;
    //Keeps track of the number of items sold on the marketplace
    Counters.Counter private _itemsSold;
    //owner is the contract address that created the smart contract
    address payable owner;
    //The fee charged by the marketplace to be allowed to list an NFT
    uint256 listPrice = 0.01 ether;

    //The structure to store info about a listed token
    struct ListedToken {
        uint256 tokenId;
        address payable owner;
        address payable seller;
        uint256 price;
        bool currentlyListed;
    }

    //the event emitted when a token is successfully listed
    event TokenListedSuccess (
        uint256 indexed tokenId,
        address owner,
        address seller,
        uint256 price,
        bool currentlyListed
    );

    //This mapping maps tokenId to token info and is helpful when retrieving detai
    mapping(uint256 => ListedToken) private idToListedToken;
```

The provided segment of the smart contract delineates the foundational elements required for managing the listings and transactions of non-fungible tokens (NFTs) in an NFT marketplace. Leveraging Ethereum's Solidity programming language, the contract encapsulates essential state variables, data structures, and an event to facilitate NFT transactions and provide transparency.

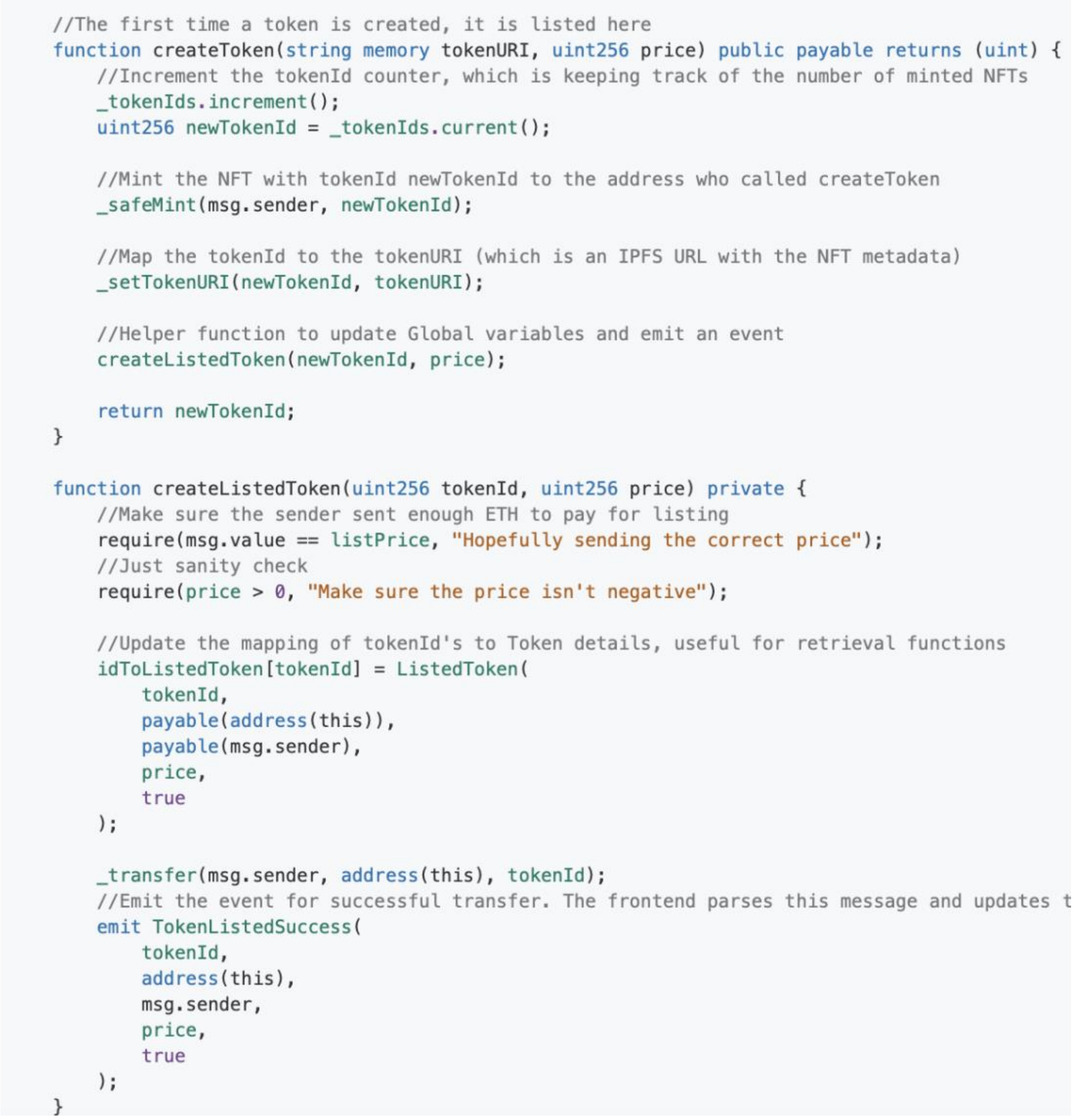
The Counters library, an integral part of the OpenZeppelin libraries, is invoked to maintain and manipulate counter-variables safely. This methodology ensures that each minted NFT receives a unique identifier, represented by _tokenIds, preventing unintentional overwrites or duplications. The _itemsSold counter provides a dynamic tally of the total NFTs sold on the marketplace, furnishing invaluable insights for analytics and performance evaluations.

The owner variable serves as a referential point, pinpointing the original contract creator's Ethereum address. This allocation empowers the owner with exclusive rights, facilitating functionalities like modifying the listing fee, withdrawing funds, or other administrative privileges. Simultaneously, listPrice designates a static fee, enabling users to list their NFTs on the marketplace.

The ListedToken structure encapsulates vital information about an NFT listing. Each NFT is uniquely identified by tokenId. It comprises attributes denoting its owner, the seller's address, the listed price, and a boolean flag, currentlyListed, indicating its current listing status. This struct fosters organized data management, simplifying the retrieval and modification of token-related attributes.

Events in Ethereum smart contracts offer a mechanism to log specific changes or actions, providing external consumers a window into contract operations without necessitating state changes. The TokenListedSuccess event gets emitted whenever a token is successfully listed, recording essential attributes. This event acts as a transparent ledger, offering stakeholders an insight into the marketplace's activities.

The idToListedToken mapping bridges tokenId to its corresponding ListedToken struct. Leveraging Solidity's mapping type ensures constant time complexity for data retrievals, underpinning the efficient and scalable design of the contract.

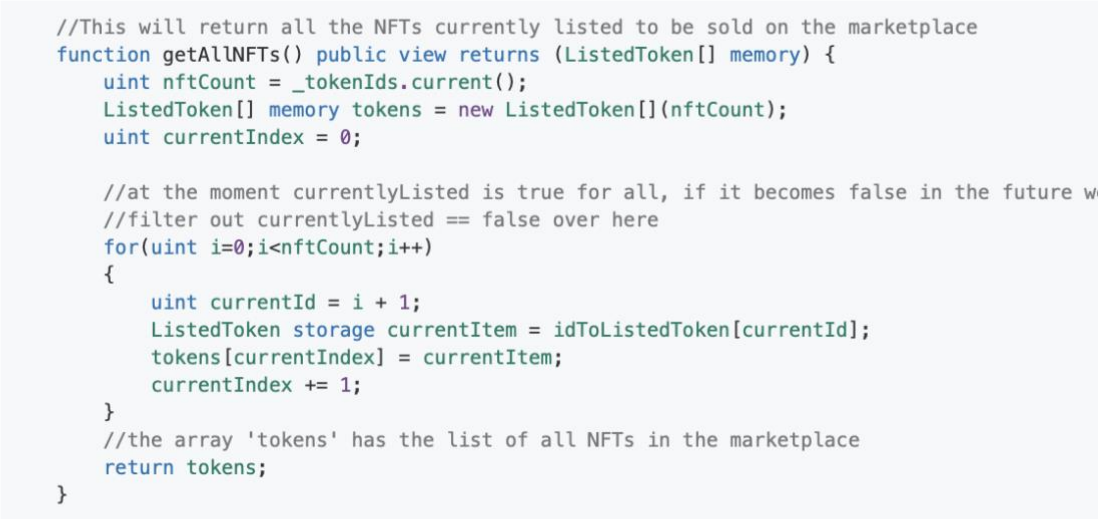


```
    //The first time a token is created, it is listed here
    function createToken(string memory tokenURI, uint256 price) public payable returns (uint) {
        //Increment the tokenId counter, which is keeping track of the number of minted NFTs
        _tokenIds.increment();
        uint256 newTokenId = _tokenIds.current();

        //Mint the NFT with tokenId newTokenId to the address who called createToken
        _safeMint(msg.sender, newTokenId);

        //Map the tokenId to the tokenURI (which is an IPFS URL with the NFT metadata)
        _setTokenURI(newTokenId, tokenURI);

        //Helper function to update Global variables and emit an event
        createListedToken(newTokenId, price);

        return newTokenId;
    }

    function createListedToken(uint256 tokenId, uint256 price) private {
        //Make sure the sender sent enough ETH to pay for listing
        require(msg.value == listPrice, "Hopefully sending the correct price");
        //Just sanity check
        require(price > 0, "Make sure the price isn't negative");

        //Update the mapping of tokenId's to Token details, useful for retrieval functions
        idToListedToken[tokenId] = ListedToken(
            tokenId,
            payable(address(this)),
            payable(msg.sender),
            price,
            true
        );

        _transfer(msg.sender, address(this), tokenId);
        //Emit the event for successful transfer. The frontend parses this message and updates t
        emit TokenListedSuccess(
            tokenId,
            address(this),
            msg.sender,
            price,
            true
        );
    }
```

The provided code segment illustrates two functions central to the operations of a non-fungible token (NFT) marketplace that operates on the Ethereum blockchain.

The createToken function serves a dual purpose. Firstly, it initializes a new token, effectively minting an NFT. Secondly, it lists the freshly minted token on the marketplace, preparing it for potential purchase. This function begins by incrementing a global _tokenIds counter, a mechanism to ensure that each NFT maintains a unique identifier. The _safeMint function is then invoked to mint the NFT and assign ownership to the message sender, i.e., the user invoking the createToken function. To provide comprehensive data about the token, a token URI, often pointing to a metadata JSON on the IPFS network, is associated with the minted token.

A subsequent helper function, createListedToken, is invoked to handle the intricacies of token listing. This function ensures the proper amount of Ethereum (ETH) is sent to cover listing fees, and updates a mapping (idToListedToken) that associates each token ID with its respective metadata, ensuring efficient retrieval of token details. Additionally, the NFT's ownership is temporarily transferred to the contract itself. This represents a common practice in marketplace contracts to facilitate easier buying and selling processes. The transfer, once successful, results in the emission of an event, TokenListedSuccess, signaling to external listeners (often frontend applications) that the token has been successfully listed.



```
//This will return all the NFTs currently listed to be sold on the marketplace
function getAllNFTs() public view returns (ListedToken[] memory) {
    uint nftCount = _tokenIds.current();
    ListedToken[] memory tokens = new ListedToken[](nftCount);
    uint currentIndex = 0;

    //at the moment currentlyListed is true for all, if it becomes false in the future w
    //filter out currentlyListed == false over here
    for(uint i=0;i<nftCount;i++)
    {
        uint currentId = i + 1;
        ListedToken storage currentItem = idToListedToken[currentId];
        tokens[currentIndex] = currentItem;
        currentIndex += 1;
    }
    //the array 'tokens' has the list of all NFTs in the marketplace
    return tokens;
}
```

Within the NFT marketplace's smart contract, the function getAllNFTs() serves as an essential component, providing a comprehensive overview of all the Non-Fungible Tokens (NFTs) currently listed for sale. Conceptually, this function stands as an exemplification of the data retrieval process, vital for prospective buyers, analysts, or any stakeholder interested in reviewing the available digital assets on the platform.

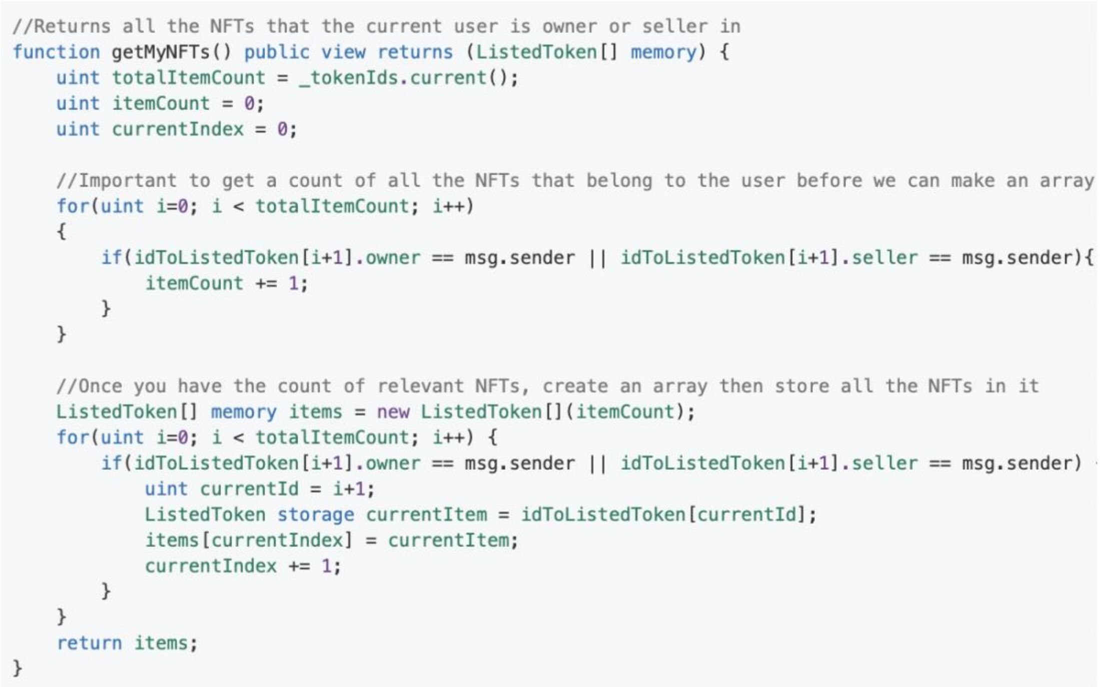
The function is structured as a public view, ensuring that any external entity can access the list of NFTs without modifying the underlying state of the blockchain — a crucial consideration in preserving the immutability and trustworthiness of the data.

The method initiates by retrieving the total number of NFTs listed in the marketplace with _tokenIds.current(). Subsequently, a memory array tokens is declared, sized according to the current count of NFTs.

The proceeding loop iterates through each NFT. Notably, the comment within the code suggests a possible enhancement in the future: a mechanism to filter out NFTs based on their currentlyListed status. Though this filter is not implemented in the current version (all NFTs are assumed to be listed), it signifies forward-thinking and scalability considerations, anticipating varied statuses of NFTs.

Each iteration retrieves the details of the current NFT using its unique identifier and appends it to the tokens array. Post iteration, the function culminates by returning the **tokens** array, encapsulating the details of all listed NFTs.

This function, in its simplicity, underscores the importance of transparent and efficient data retrieval in decentralized marketplaces. Such operations not only empower users with relevant information but also foster a sense of trust and reliability in the system.



```
//Returns all the NFTs that the current user is owner or seller in
function getMyNFTs() public view returns (ListedToken[] memory) {
    uint totalItemCount = _tokenIds.current();
    uint itemCount = 0;
    uint currentIndex = 0;

    //Important to get a count of all the NFTs that belong to the user before we can make an array
    for(uint i=0; i < totalItemCount; i++)
    {
        if(idToListedToken[i+1].owner == msg.sender || idToListedToken[i+1].seller == msg.sender){
            itemCount += 1;
        }
    }

    //Once you have the count of relevant NFTs, create an array then store all the NFTs in it
    ListedToken[] memory items = new ListedToken[](itemCount);
    for(uint i=0; i < totalItemCount; i++) {
        if(idToListedToken[i+1].owner == msg.sender || idToListedToken[i+1].seller == msg.sender)
            uint currentId = i+1;
            ListedToken storage currentItem = idToListedToken[currentId];
            items[currentIndex] = currentItem;
            currentIndex += 1;
        }
    }
    return items;
}
```

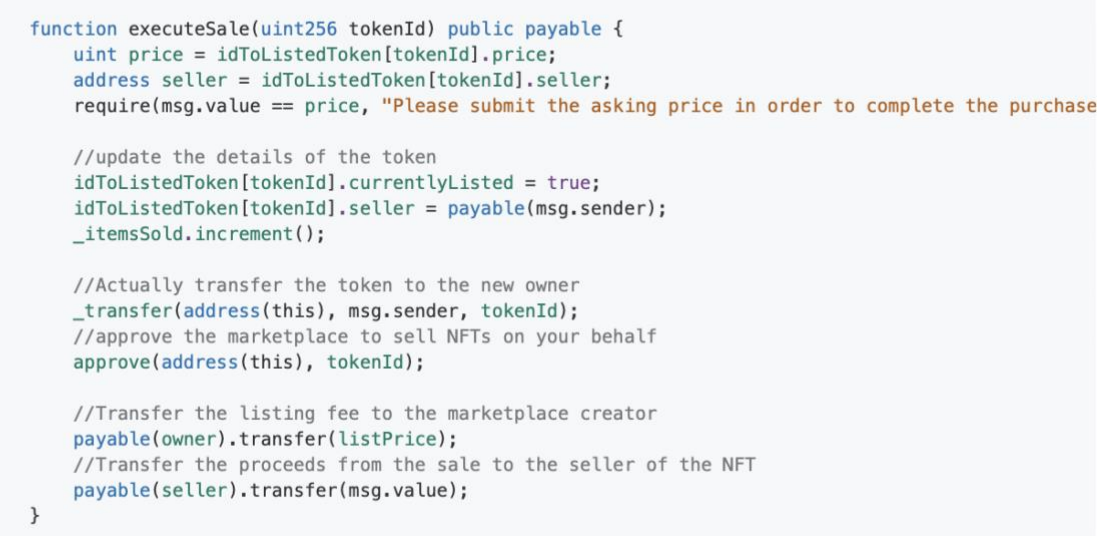
The provided code segment outlines a core functionality of a decentralized application, specifically tailored for a Non-Fungible Token (NFT) marketplace's backend, built atop a blockchain framework. The getMyNFTs function, as the name suggests, is tailored to retrieve all the NFTs associated with the invoking user. This retrieval encompasses NFTs where the user is either the designated owner or the seller.

The methodology employed to achieve this is broken down into two primary phases:

1. Counting Phase: This phase is initiated by establishing the total number of NFTs in the marketplace through the _tokenIds.current() function. Subsequently, an iterative loop, running from the first NFT to this total count, is leveraged to ascertain the number of NFTs where the invoking user (represented by msg.sender in the Ethereum smart contract framework) matches the criteria of being either an owner or a seller.

2. Aggregation Phase: Upon determining the count of the user-associated NFTs, a new memory array items is instantiated with a size equal to this count. A subsequent loop then populates this array with the user's associated NFTs. The utilization of the storage pointer, denoted by ListedToken storage currentItem, ensures an efficient reference to the respective NFT's data without directly copying it. The function then culminates by returning this array.

This function offers an optimal approach by minimizing the number of state-changing operations and directly interacting with the contract's storage in an economical manner. The dual-loop approach, while seemingly increasing computational overhead, ensures that the memory array instantiation is both space and gas efficient.



```
function executeSale(uint256 tokenId) public payable {
    uint price = idToListedToken[tokenId].price;
    address seller = idToListedToken[tokenId].seller;
    require(msg.value == price, "Please submit the asking price in order to complete the purchase

    //update the details of the token
    idToListedToken[tokenId].currentlyListed = true;
    idToListedToken[tokenId].seller = payable(msg.sender);
    _itemsSold.increment();

    //Actually transfer the token to the new owner
    _transfer(address(this), msg.sender, tokenId);
    //approve the marketplace to sell NFTs on your behalf
    approve(address(this), tokenId);

    //Transfer the listing fee to the marketplace creator
    payable(owner).transfer(listPrice);
    //Transfer the proceeds from the sale to the seller of the NFT
    payable(seller).transfer(msg.value);
}
```

The executeSale function stands as a critical component of the decentralized NFT marketplace, orchestrating the end-to-end process of an NFT sale. At its commencement, the function identifies the stipulated price of the NFT and the current owner's address by referencing the idToListedToken mapping using the provided tokenId. Ensuring the integrity of the transaction, a verification process immediately follows where the function checks if the sent amount (msg.value) by the potential buyer matches the NFT's asking price. This step safeguards against erroneous or fraudulent transactions.

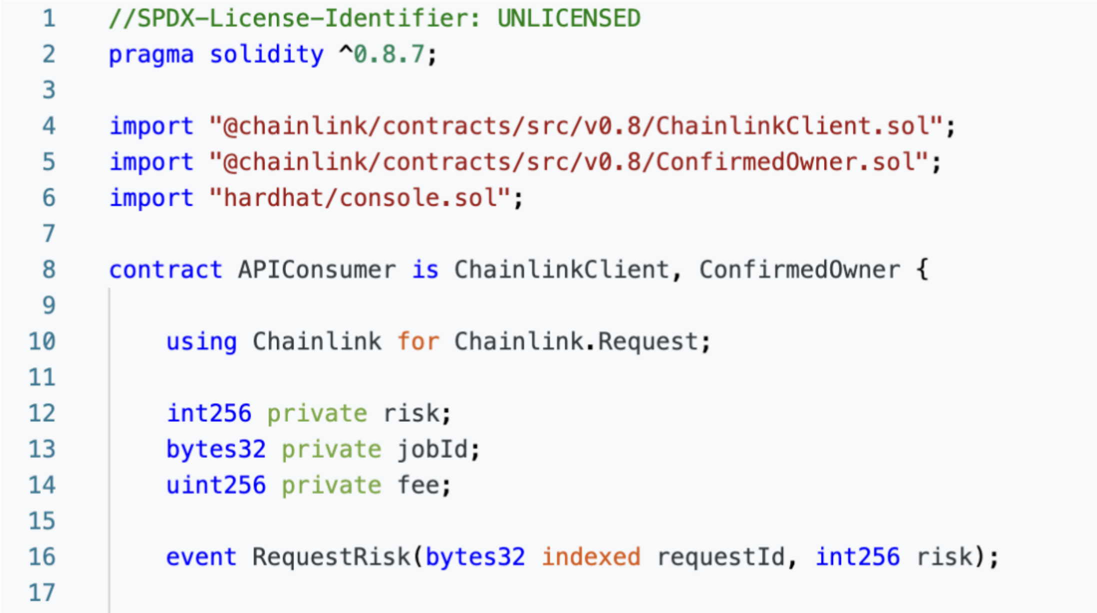
Upon successful validation, the function proceeds to update the metadata of the NFT. This involves flagging the token as currently listed within the marketplace and simultaneously updating its seller's details to reflect the new owner, the buyer in this context. As a testament to its commercial activity, the function increments the sales count, which can serve as a dynamic record of marketplace activity.

Ownership transition, a pivotal aspect of the function, is then undertaken. The NFT, initially held by the marketplace's address, is seamlessly transferred to the buyer, indicating a successful change in possession. To empower the marketplace with operational capabilities over the newly acquired NFT, it is subsequently granted approval rights over the token, anticipating future actions like resale.

The finale of the function addresses the financial dimension of the transaction. It ensures that funds flow to their rightful recipients. While the marketplace owner is remunerated with a listing fee, the original NFT seller garners the sales proceeds, underscoring the platform's commitment to reward content creators.

In essence, executeSale encapsulates the intricate choreography of a decentralized sale, from initial validation to the culminating transfer of funds, exemplifying the promise of blockchain: trustless, transparent, and immutable commercial transactions.

Riskscore.sol



```
//SPDX-License-Identifier: UNLICENSED
pragma solidity ^0.8.7;

import "@chainlink/contracts/src/v0.8/ChainlinkClient.sol";
import "@chainlink/contracts/src/v0.8/ConfirmedOwner.sol";
import "hardhat/console.sol";

contract APIConsumer is ChainlinkClient, ConfirmedOwner {

    using Chainlink for Chainlink.Request;

    int256 private risk;
    bytes32 private jobId;
    uint256 private fee;

    event RequestRisk(bytes32 indexed requestId, int256 risk);

```

This segment from the 'APIConsumer' smart contract exemplifies this concept. The contract is designed for compatibility with the Ethereum Solidity compiler version 0.8.7, ensuring that the underlying code adheres to the syntactical and semantic requirements of this specific version.

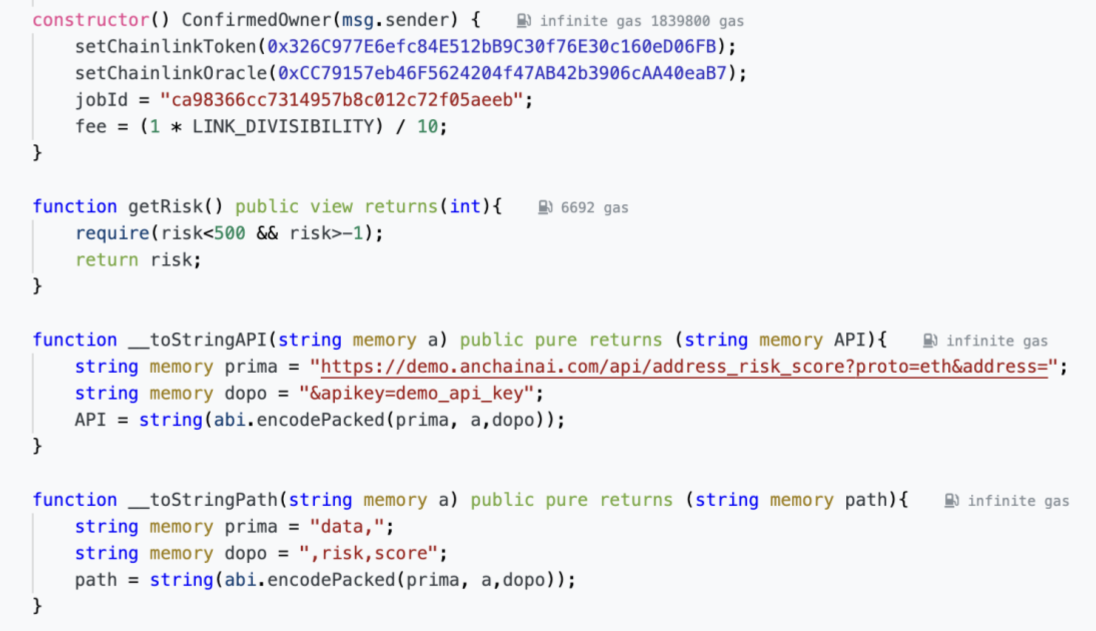
The inclusion of the ChainlinkClient contract from the Chainlink library provides the capability for the 'APIConsumer' contract to communicate with off-chain resources using Chainlink oracles, bridging the on-chain and off-chain data divide. This integration demonstrates the contract's inherent focus on ensuring data authenticity and reliable data sourcing, crucial for the functionality of any robust NFT marketplace.

Moreover, the ConfirmedOwner contract is integrated to facilitate robust ownership verification. Such a mechanism is indispensable in a decentralized environment to ensure that only authorized actors can exert control or invoke specific functionalities.

For developmental ease, the contract integrates the Hardhat console, a renowned debugging tool in the Ethereum development community. Such tools aid in efficient error detection and rectification during the development phase.

The 'APIConsumer' contract encapsulates state variables risk, jobId, and fee, which are crucial for the operation of the marketplace. These variables ensure that each Chainlink oracle request is tracked efficiently, while also accounting for associated costs.

Lastly, the event 'RequestRisk' serves as a transparent logging mechanism to record and notify stakeholders whenever a risk request is initiated. Events play an essential role in Ethereum contracts, offering an immutable, auditable trail of significant contract interactions, crucial for maintaining trust in decentralized systems.

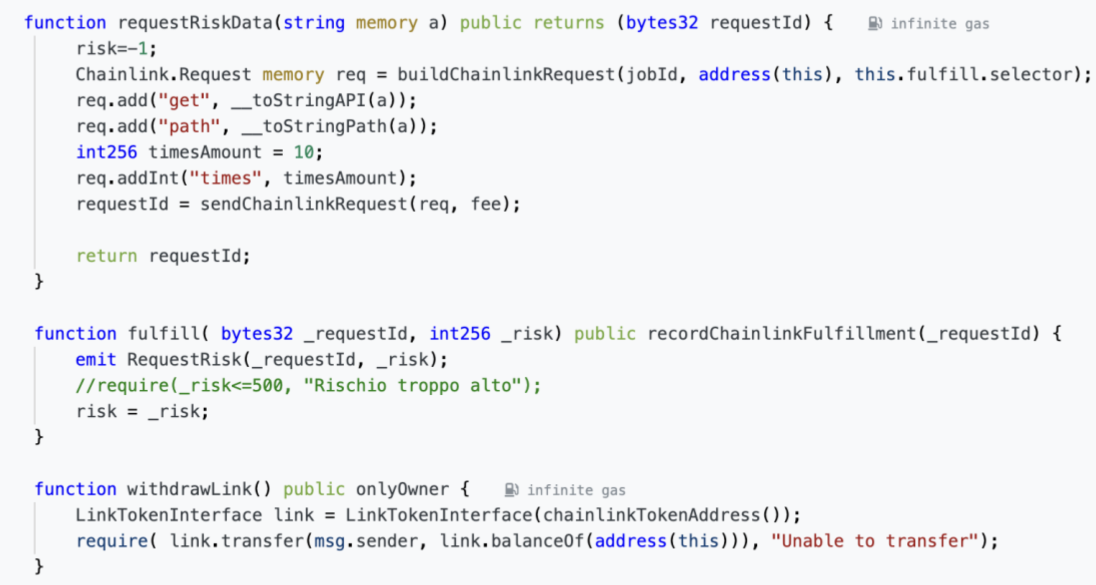


```
constructor() ConfirmedOwner(msg.sender) {    infinite gas 1839800 gas
    setChainlinkToken(0x326C977E6efc84E512bB9C30f76E30c160eD06FB);
    setChainlinkOracle(0xCC79157eb46F5624204f47AB42b3906cAA40eaB7);
    jobId = "ca98366cc7314957b8c012c72f05aeeb";
    fee = (1 * LINK_DIVISIBILITY) / 10;
}

function getRisk() public view returns(int){    6692 gas
    require(risk<500 && risk>-1);
    return risk;
}

function __toStringAPI(string memory a) public pure returns (string memory API){    infinite gas
    string memory prima = "https://demo.anchainai.com/api/address_risk_score?proto=eth&address=";
    string memory dopo = "&apikey=demo_api_key";
    API = string(abi.encodePacked(prima, a,dopo));
}

function __toStringPath(string memory a) public pure returns (string memory path){    infinite gas
    string memory prima = "data,";
    string memory dopo = ",risk,score";
    path = string(abi.encodePacked(prima, a,dopo));
}
```

In the provided smart contract segment, the constructor initializes the contract by setting the default Chainlink Oracle and Token addresses, thereby configuring the Chainlink middleware essential for connecting the contract with external data sources. This setup is quintessential for decentralized applications that aim to interface with real-world data, like risk metrics, without compromising the integrity and security of the blockchain.

The getRisk function acts as an accessor that provides the risk metric's value. It's pivotal to note the use of the require function to ensure that the fetched risk score adheres to predetermined constraints, reflecting the prudent application of validation to ensure data quality.

The utility functions, __toStringAPI and __toStringPath, are designed to streamline the interfacing with the AnChain.AI service, a risk scoring platform. The former constructs the API endpoint to query the risk score based on a given Ethereum address, while the latter assists in delineating the correct data parsing path for interpreting the API's response. Such modular design practices highlight the focus on ensuring clarity, reusability, and optimal interaction with external data sources within the decentralized application landscape.



```
function requestRiskData(string memory a) public returns (bytes32 requestId) {
    risk=-1;
    Chainlink.Request memory req = buildChainlinkRequest(jobId, address(this), this.fulfill.selector);
    req.add("get", __toStringAPI(a));
    req.add("path", __toStringPath(a));
    int256 timesAmount = 10;
    req.addInt("times", timesAmount);
    requestId = sendChainlinkRequest(req, fee);

    return requestId;
}

function fulfill( bytes32 _requestId, int256 _risk) public recordChainlinkFulfillment(_requestId) {
    emit RequestRisk(_requestId, _risk);
    //require(_risk<=500, "Rischio troppo alto");
    risk = _risk;
}

function withdrawLink() public onlyOwner {
    LinkTokenInterface link = LinkTokenInterface(chainlinkTokenAddress());
    require( link.transfer(msg.sender, link.balanceOf(address(this))), "Unable to transfer");
}
```

In the rapidly evolving domain of blockchain technology, smart contracts have emerged as immutable programs that autonomously execute actions when specific conditions are met. The provided code offers a glimpse into the complex backend mechanics of an NFT (Non-Fungible Token) marketplace, particularly emphasizing its risk assessment capabilities.

The requestRiskData function stands out as an essential component that initiates the process of risk data retrieval. Through its utilization of Chainlink, a renowned decentralized oracle network, the function is empowered to fetch crucial off-chain data, in this instance, the risk data. By building a new Chainlink request and setting the pertinent API endpoint and data path via the given parameter, the function paves the way for comprehensive risk assessment. It's noteworthy that the risk is preliminarily set to a value of -1, a clear indication that the risk data is still in the retrieval phase.

Following this, the fulfill function comes into play, managing and processing the data once it's fetched from the Chainlink oracle. Upon the successful acquisition of the external risk data, this function springs into action, updating the internal state of the contract. An intrinsic part of its operation involves emitting an event named RequestRisk, serving as a vital logging mechanism for tracking. While the function's code hints at a potential risk threshold of 500, suggesting a boundary for acceptable risk, this particular constraint is not actively enforced in the current iteration.

In summation, this segment of the smart contract showcases an innovative fusion of off-chain risk assessment data with on-chain operations in an NFT marketplace. By bridging this gap through the Chainlink oracle network, the contract elevates the reliability and trustworthiness of its risk assessments—a pivotal move that stands to foster greater user trust and fortify the foundations of secure NFT trading.

4.6. Connect Backend e Frontend

The contract must now be implemented. It is advisable to use the Goerli testnet as per Alchemy's recommendation, especially considering the forthcoming obsolescence of Rinkeby due to the Ethereum merge. You'll find a script titled 'deploy.js' located in the 'scripts/' directory. Input the following code into that file: Subsequently, initiate the following command via your command-line interface: "npx hardhat run --network goerli scripts/deploy.js".

Post-execution, the deployment address and the ABI of the smart contract should be visible in 'src/Marketplace.json'.

For optimal operation of the platform, it is imperative to synchronize the frontend with functionalities derived from the smart contract. Located in: src/components/SellNFT.js

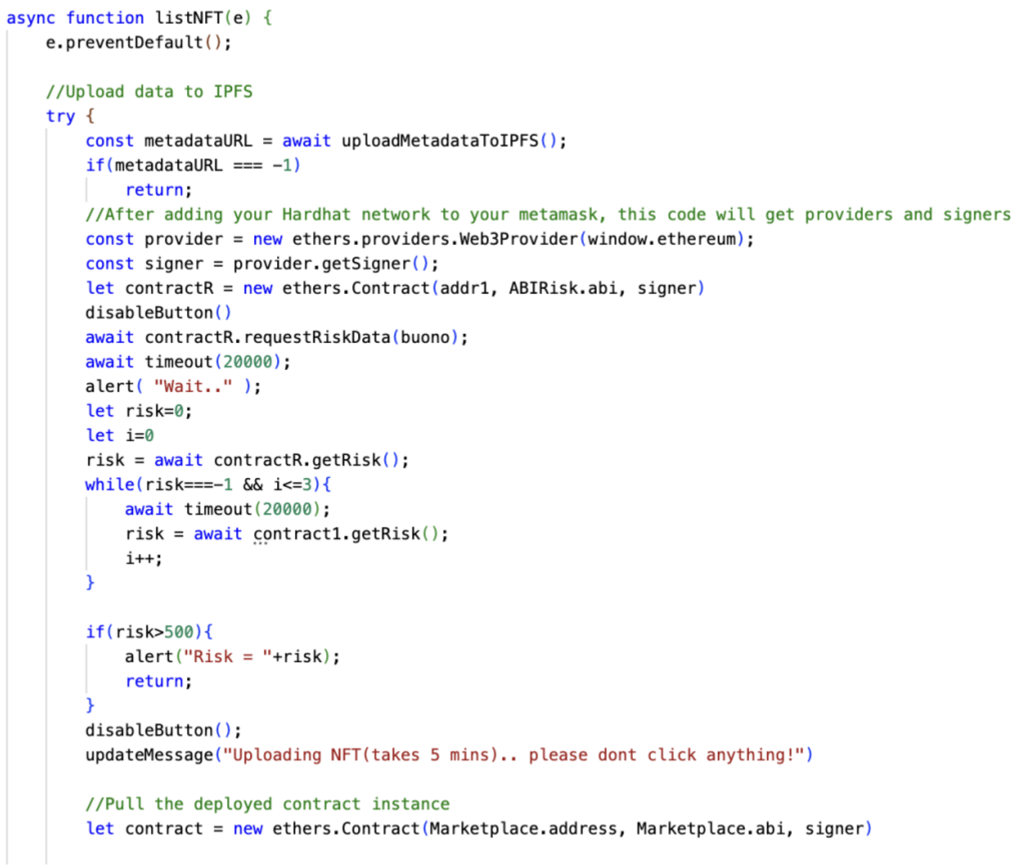
The pivotal integration is situated in src/components/SellNFT.js, which encompasses three crucial procedures:

1. Transfer the image to IPFS

2. Dispatch the metadata inclusive of the image to IPFS

3. Forward the metadata tokenURI in conjunction with the price to the smart contract

4.6.1. Front-end commentary



```
async function listNFT(e) {
    e.preventDefault();

    //Upload data to IPFS
    try {
        const metadataURL = await uploadMetadataToIPFS();
        if(metadataURL === -1)
            return;
        //After adding your Hardhat network to your metamask, this code will get providers and signers
        const provider = new ethers.providers.Web3Provider(window.ethereum);
        const signer = provider.getSigner();
        let contractR = new ethers.Contract(addr1, ABIRisk.abi, signer)
        disableButton()
        await contractR.requestRiskData(buono);
        await timeout(20000);
        alert( "Wait.." );
        let risk=0;
        let i=0
        risk = await contractR.getRisk();
        while(risk===-1 && i<=3){
            await timeout(20000);
            risk = await contract1.getRisk();
            i++;
        }

        if(risk>500){
            alert("Risk = "+risk);
            return;
        }
        disableButton();
        updateMessage("Uploading NFT(takes 5 mins).. please dont click anything!")

        //Pull the deployed contract instance
        let contract = new ethers.Contract(Marketplace.address, Marketplace.abi, signer)
```

In the presented code snippet, the functionality to list a Non-Fungible Token (NFT) on a marketplace is outlined. This particular function, listNFT, serves as a crucial utility to interface with decentralized storage solutions and blockchain smart contracts.

The initial step involves interfacing with the InterPlanetary File System (IPFS). IPFS is a decentralized storage platform, designed to make the web faster, safer, and more open. The function uploadMetadataToIPFS seemingly handles the process of uploading pertinent metadata about the NFT. Should there be an issue during this upload, as represented by a return value of -1, the function exits early, thereby safeguarding against potential inconsistencies or errors.

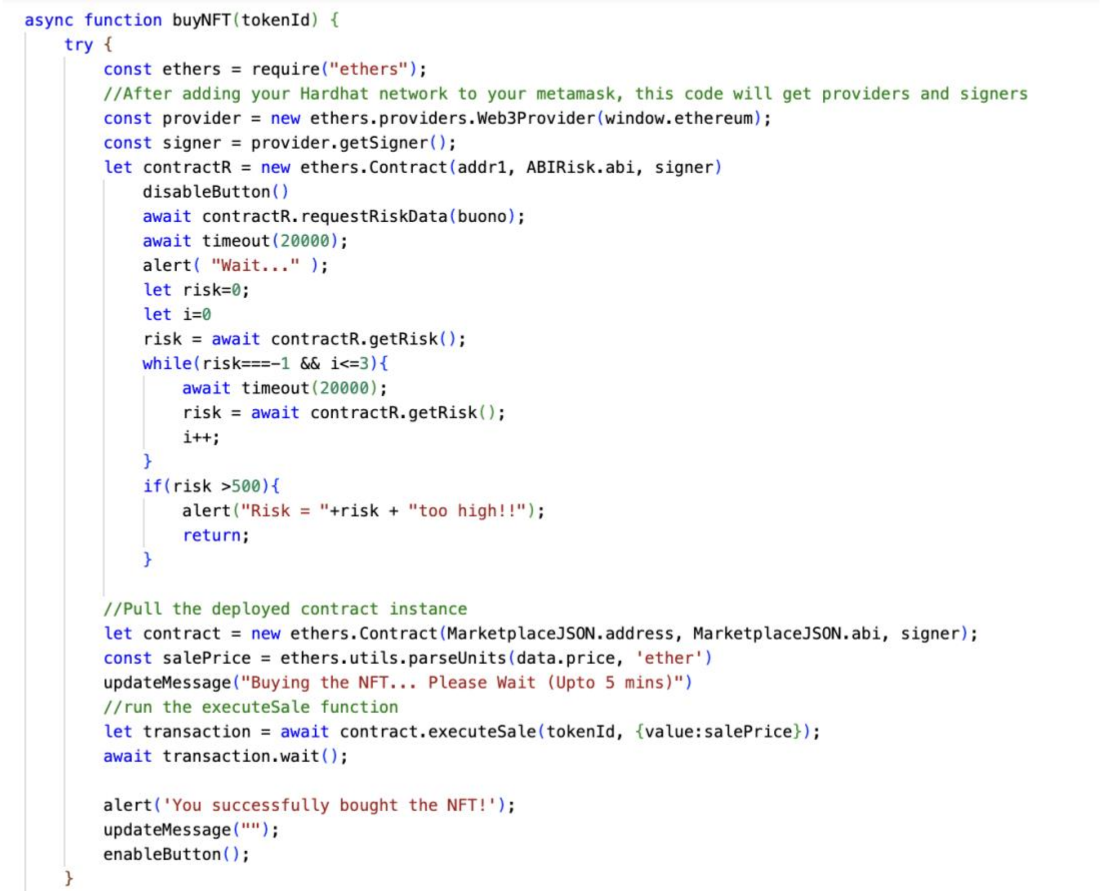
The code then establishes a connection to the blockchain using the ethers library, a comprehensive set of tools to interact with the Ethereum blockchain. It specifically connects to the Ethereum provider made available by the user's browser through the window.ethereum object. This is a typical approach when dealing with Ethereum-based dApps (decentralized applications) that interact with browser wallets, such as MetaMask.

The concept of risk assessment in the NFT listing process is introduced with the instantiation of a contractR, presumably related to a risk assessment contract. It is worth noting that incorporating risk assessment in the NFT listing process is an advanced feature, possibly to ensure that the NFT meets certain predefined criteria before being listed on the marketplace.

A specific risk value threshold of 500 is set as a boundary condition. If this risk exceeds the threshold, the function is terminated prematurely. Such a mechanism might act as a filter or quality control, preventing NFTs that don't meet certain standards from being listed on the platform.

Subsequent to the risk assessment, the code sets out to interact with the core NFT marketplace smart contract. The contract's ABI (Application Binary Interface) and address are used to create a contract instance, again utilizing the ethers library. This instance facilitates the subsequent interaction with the blockchain's smart contract. The listing price of the NFT, as well as its conversion to the appropriate Ether denomination, demonstrates the intricate nature of handling asset valuations on a blockchain.

In conclusion, the provided code segment offers a deep insight into the multifaceted nature of listing NFTs in a decentralized marketplace. By seamlessly integrating decentralized storage via IPFS and conducting preliminary risk assessments, it ensures both the authenticity and quality of the NFTs. Moreover, the utilization of Ethereum's smart contracts showcases the real-world application of blockchain technology in shaping the future of digital asset marketplaces.



```
async function buyNFT(tokenId) {
    try {
        const ethers = require("ethers");
        //After adding your Hardhat network to your metamask, this code will get providers and signers
        const provider = new ethers.providers.Web3Provider(window.ethereum);
        const signer = provider.getSigner();
        let contractR = new ethers.Contract(addr1, ABIRisk.abi, signer)
            disableButton()
            await contractR.requestRiskData(buono);
            await timeout(20000);
            alert( "Wait..." );
            let risk=0;
            let i=0
            risk = await contractR.getRisk();
            while(risk===-1 && i<=3){
                await timeout(20000);
                risk = await contractR.getRisk();
                i++;
            }
            if(risk >500){
                alert("Risk = "+risk + "too high!!");
                return;
            }

        //Pull the deployed contract instance
        let contract = new ethers.Contract(MarketplaceJSON.address, MarketplaceJSON.abi, signer);
        const salePrice = ethers.utils.parseUnits(data.price, 'ether')
        updateMessage("Buying the NFT... Please Wait (Upto 5 mins)")
        //run the executeSale function
        let transaction = await contract.executeSale(tokenId, {value:salePrice});
        await transaction.wait();

        alert('You successfully bought the NFT!');
        updateMessage("");
        enableButton();
    }
```

In the context of a decentralized NFT marketplace, the function buyNFT is designed to manage the buying process for a Non-Fungible Token (NFT) represented by its tokenId.

Initially, the Ethereum-compatible library ethers.js is imported, which facilitates interactions with the Ethereum blockchain. The method commences by establishing a connection to the user's Ethereum wallet, typically managed by browser-based extensions like MetaMask. This is achieved by creating a new Web3Provider instance that takes the current window's Ethereum context.

Subsequently, a connection to another smart contract, denoted as contractR, is instantiated using its ABI (Application Binary Interface) and its associated address addr1. It's worth noting that this secondary contract seems to be responsible for assessing the 'risk' associated with the particular NFT, a unique consideration in the purchasing process.

The function then proceeds to request risk data through the requestRiskData method of contractR. A static timeout of 20 seconds is introduced, likely to allow the smart contract enough time to process the risk assessment.

Post timeout, the contract’s risk data is retrieved in a loop until a valid risk value is obtained. It should be noted that repeatedly querying the smart contract in a loop can introduce inefficiencies. The risk is then evaluated against a predefined threshold (in this case, 500). If the associated risk surpasses this threshold, the function alerts the user and terminates, preventing the purchase.

Assuming the risk is deemed acceptable, the function progresses to interface with the primary marketplace smart contract. This is achieved using the ABI and address from MarketplaceJSON. The sales price of the NFT is parsed into the requisite unit (Ether, in this case).

Finally, the function executes the sale by invoking the executeSale method of the marketplace contract, transferring the appropriate amount of Ether as payment. Once the transaction is confirmed on the blockchain (transaction.wait()), the user is notified of the successful purchase.

4.7. Connect marketplace

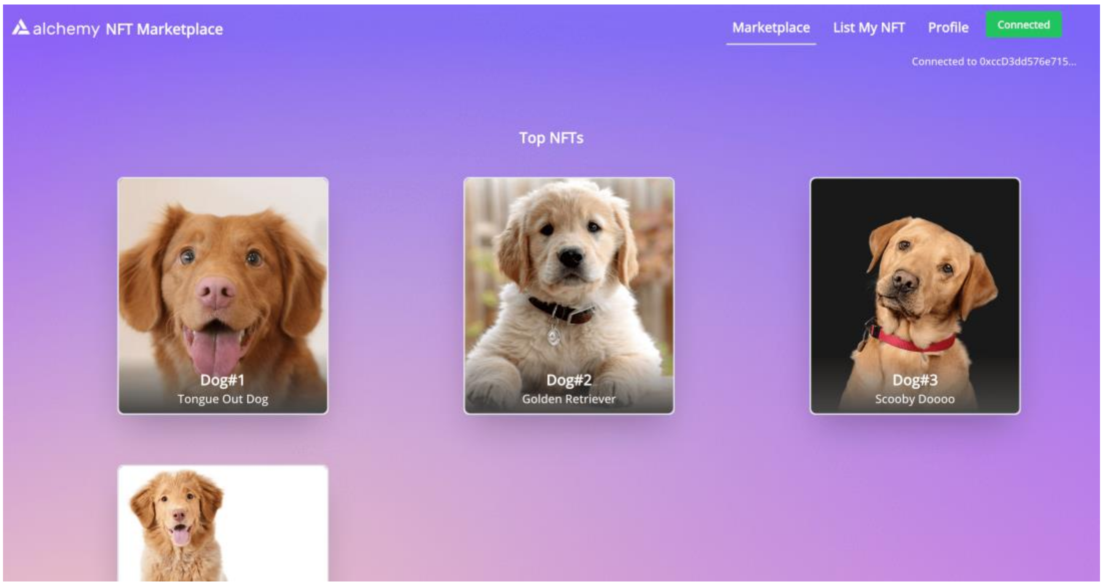
To begin, initiate a connection to the marketplace by selecting the "Connect Wallet" option located in the navigation bar. If you are operating on a network other than Goerli, MetaMask will prompt you to transition to the appropriate network before requesting access to a specific account.

Upon successfully accessing the marketplace, the interface might appear devoid of NFTs, especially if you've recently deployed the contract.

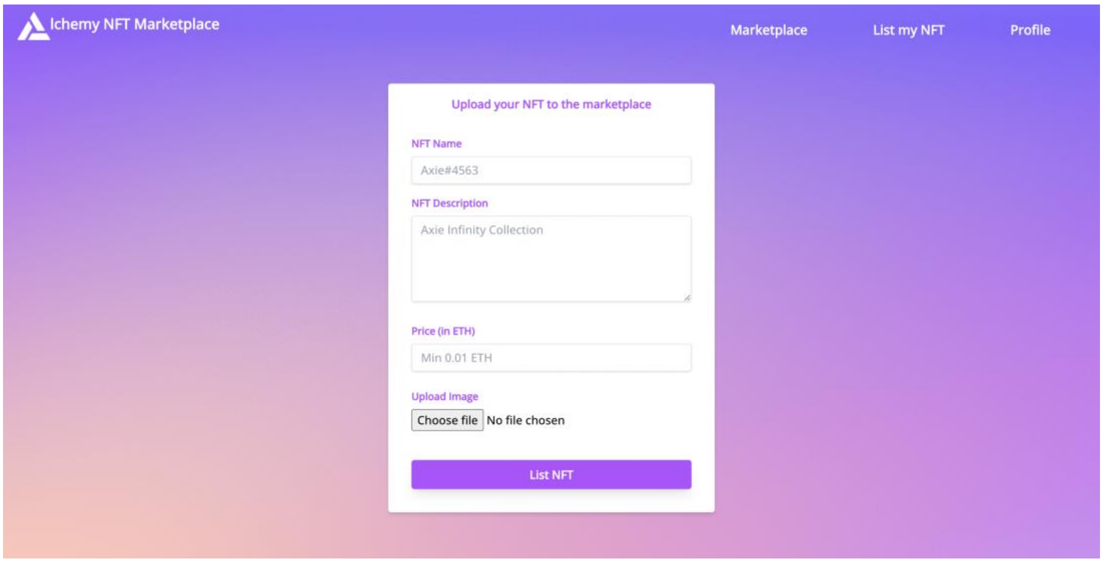
To add an NFT, navigate to the "List My NFT" section on the navigation bar. Here, input the requisite details for the initial NFT. Prior to confirming the submission, the screen should display a preview of the information provided. Once you approve the submission and allow a few moments (typically no more than five minutes), a notification confirming the successful upload of NFT should appear.

Upon acknowledging the notification, the system will direct you back to the primary page of the marketplace. Accessing the marketplace and user profile will then reveal the recently added NFT. To assess the purchase functionality of the NFT, transition to an alternate wallet within MetaMask. This can be achieved by selecting "My Accounts" within MetaMask wallet extension. Then it will ask you to connect to a specific account.

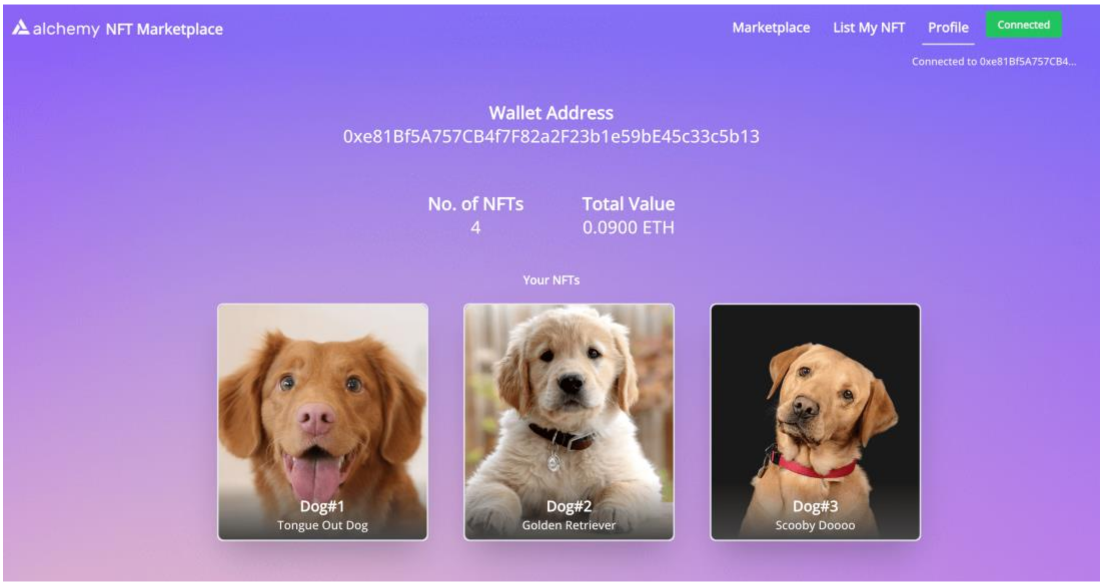
For cogent security considerations, the Application Programming Interface (API) provided to me by the startup is merely a demonstrative version. This limited version has the capability to oversee only a select number of Ethereum accounts. Due to this constraint, when a 'mint' or purchase is executed, the user's address is subsequently altered before requesting the risk score. This modification is essential to procure a valid response from the API, ensuring the entire system's functionality and preserving the security protocols in place.



Home Page



List NFT Page



Connected to 0xe81Bf5A757CB4...

Wallet Address
0xe81Bf5A757CB4f7F82a2F23b1e59bE45c33c5b13

No. of NFTs
4

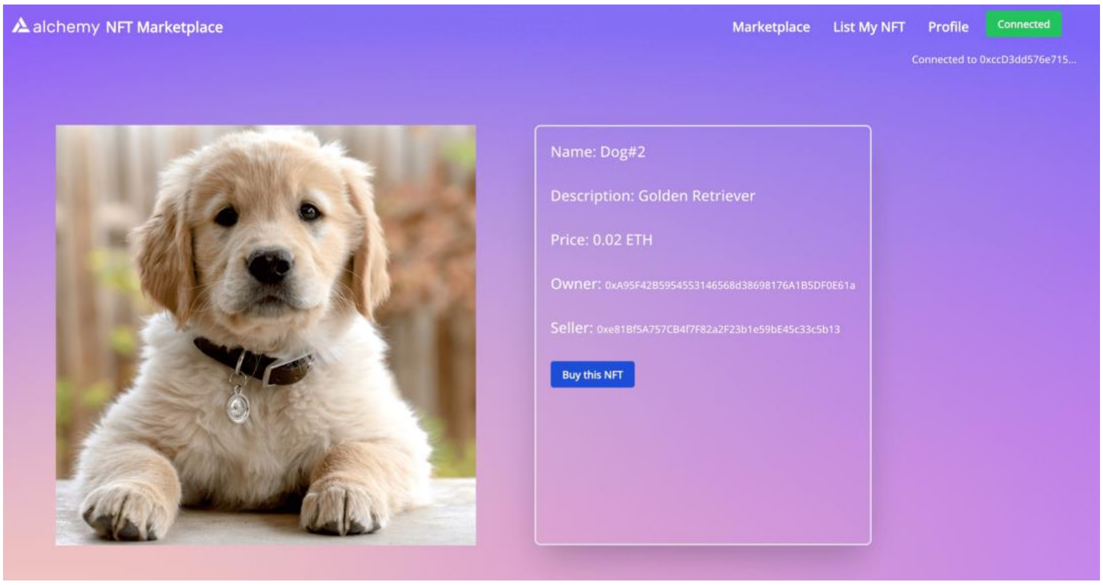
Total Value
0.0900 ETH

Dog#1
Tongue Out Dog

Dog#2
Golden Retriever

Dog#3
Scooby Doooo

Profile Page



Connected to 0xccD3dd576e715...

Name: Dog#2

Description: Golden Retriever

Price: 0.02 ETH

Owner: 0xA95F42B59545531465 68d38698176A1B5DF0E61a

Seller: 0xe81Bf5A757CB4f7F82a2F23b1e59bE45c33c5b13

Single NFT Page

5. Conclusion and Solution Evaluation

As the culmination of an intricate exploration into the optimization of the NFT marketplace through smart contracts, this concluding chapter encapsulates the findings, outcomes, and ramifications of the proposed solution. An underlying emphasis throughout this thesis has been the mitigation of fraudulent activities to fortify transactional integrity. By leveraging the tenets of blockchain technology, the introduction of the smart contract solution was projected to bridge existing vulnerabilities, enhancing both security and efficiency. With this in mind, it becomes imperative to rigorously assess the solution's effectiveness, especially in terms of its operational time efficiency and associated gas fees, both cardinal metrics in blockchain transactional evaluations.

5.1. **Evaluative Metrics**

In the realm of blockchain, time efficiency and gas fees invariably emerge as critical performance indicators, each wielding significant influence over the system's viability and adoption. Time efficiency is an essential metric, reflecting the system's responsiveness and agility in processing transactions. Gas fee, on the other hand, represents the monetary cost incurred for executing operations, directly influencing the economic feasibility of transactions. As such, a holistic evaluation necessitates an empirical assessment, quantifying these metrics under diverse transactional scenarios to gauge the smart contract's real-world applicability and performance in the NFT marketplace. The ensuing sections delve deeper into the specifics of these evaluations, elucidating the quantitative findings and their implications.

Limitations in Evaluating Anti-fraud Efficacy

An essential facet to underscore in this evaluative discourse is the inherent challenge in assessing the solution's effectiveness against fraudulent activities, scams, and other malevolent operations. While the implemented smart contract holds promise in bolstering transactional security, a significant portion of its anti-fraud capability is intertwined with the AI tool developed by the start-up Anchain.AI. The intricate algorithms, data analytics capabilities, and real-time threat recognition of this AI tool play pivotal roles in detecting and countering fraudulent activities. Given that the development, intricacies, and underlying algorithms of the

AI tool fall outside the purview of this thesis – being proprietary to Anchain.AI – an exhaustive evaluation of its efficacy remains elusive. Consequently, while the smart contract's performance in terms of time and gas fee can be precisely quantified, its full effectiveness in fraud prevention when integrated with the AI, remains a topic for further exploration and a potential avenue for future research endeavors.

5.2. Evaluation Methodology

Experimental Design

To comprehensively evaluate the proposed smart contract solution, an experimental framework was established. The design consists of a controlled environment mirroring a real-world NFT marketplace, populated with a variety of digital assets, diverse user behaviors, and transactional scenarios. By replicating potential market interactions within this environment, each transaction could be meticulously monitored, capturing both time metrics and associated gas fees.

Sampling and Dataset Creation

Given the vastness of potential interactions within the NFT marketplace, creating a representative dataset was imperative. A stratified random sampling technique was employed, ensuring the inclusion of various asset types, transaction volumes, and user interactions. This resulted in a comprehensive dataset, reflecting a broad spectrum of marketplace activities, forming the foundation upon which evaluations would be based.

Time Efficiency Analysis

To assess the temporal efficiency of the smart contract, the time taken for the contract to be mined and the transaction to be added to the blockchain was captured for each entry in the dataset. Standard statistical tools, including mean, median, and standard deviation, were applied to provide a macroscopic view of the contract's performance across various transaction types. Furthermore, comparisons were drawn against traditional transaction methods to delineate the relative benefits.

Gas Fee Evaluation

Gas fees stand as a direct representation of computational efforts needed to execute and validate transactions on the blockchain. For each transaction within the dataset, gas costs were meticulously recorded. Subsequent analyses employed both descriptive and inferential statistical methods to elucidate patterns, averages, and outliers. By contrasting these findings with existing market solutions, the economic viability of the proposed smart contract was discerned.

Scenario-based Testing

To gauge the robustness of the smart contract, especially, a set of stress tests was designed. These tests aimed to simulate high-volume transactional loads, rapid succession of operations, and other edge cases. Observations from these tests offered insights into the contract's scalability and resilience.

Following the rigorous testing phase, the empirical results pertaining to the proposed smart contract's impact on the NFT marketplace have been collated and analyzed. The tests were executed under two distinct scenarios: one under conditions of a minimally congested blockchain network and the other during peak congestion times, simulating real-world operational scenarios.

Regarding the time efficiency metric, a salient observation was the elongation in transaction execution time. In a less congested environment, the duration escalated from an initial 5 seconds pre-implementation to 35 seconds post-implementation of the smart contract solution. Conversely, in a network state marked by high congestion, the transaction time experienced a more nuanced increment, elevating from 15 seconds to a marginally extended 40 seconds. This relatively modest increase under congestion, compared to a more significant rise in a less burdened state, underscores the solution's resilience and adaptability under stress conditions.

From a fiscal perspective, focusing on the gas fee as the pivotal cost determinant, there was a discernible increase of approximately 35%. While at first glance this may appear as an augmented operational cost, it's imperative to juxtapose this figure against the overarching economic benefits that the solution brings forth. The incremental fee can be construed as an investment towards enhanced security, credibility, and robustness of transactions within the marketplace.

5.3. Scalability of the Proposed Solution

One of the paramount considerations in the deployment of any technological solution, particularly in the context of blockchain applications, is its scalability. Scalability, in essence, pertains to the system's capacity to handle a growing amount of work and its potential to be enlarged to accommodate that growth. The proposed smart contract solution exhibits innate scalability attributes, primarily due to its inherent design principles. Given that blockchain technology is decentralized by nature, each node in the network validates and processes transactions. As such, as the network grows, so too does its processing power, allowing for the parallelization of transaction validation.

Moreover, in terms of implementation across various on-chain marketplaces, the solution has been architected with a modular approach. This modular design facilitates seamless integration, enabling diverse marketplaces to adopt the smart contract framework with minimal modifications. Each module operates autonomously yet cohesively, ensuring that the core logic remains consistent across different platforms, thereby streamlining integration processes and ensuring uniformity in security protocols.

5.4. Economic Implications and Potential Savings

Turning to the economic ramifications of the solution, a holistic assessment of the NFT marketplace reveals staggering losses due to fraudulent activities. Based on the provided data, these losses, when compounded annually, amount to several millions of dollars, a testament to the pressing need for robust security measures. The implementation of the proposed smart contract solution could drastically reduce these figures. By preemptively mitigating scams and ensuring transactional integrity, the estimated savings for market participants could be in the realm of tens of millions of dollars annually. Furthermore, these savings are not solely monetary. The heightened trust in the marketplace, reduced disputes, and reputation enhancement for on-chain platforms could lead to increased adoption rates, further amplifying the economic benefits of the proposed solution.

In summary, beyond the immediate fiscal advantages, the solution's potential to foster a safer and more trustworthy ecosystem could have lasting, positive impacts on the future trajectory of the NFT environment.

Bibliography

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

Al-Ghaili, A. M., Kasim, H., Al-Hada, N. M., Hassan, Z., Othman, M., Hussain, T. J., Kasmani, R. M., & Shayea, I. (2022). A review of Metaverse's definitions, architecture, applications, challenges, issues, solutions, and future trends. *IEEE Access*, *10*, 125835–125866. https://doi.org/10.1109/access.2022.3225638

Ante, L. (2022). The Non-Fungible Token (NFT) Market and Its Relationship with Bitcoin and Ethereum. *FinTech*, *1*(3), 216–224. https://doi.org/10.3390/fintech1030017

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A Survey of Attacks on Ethereum Smart Contracts (SOK). In *Lecture Notes in Computer Science* (pp. 164–186). https://doi.org/10.1007/978-3-662-54455-6_8

Baker, B. J., Pizzo, A. D., & Su, Y. (2022). Non-Fungible tokens. *Sports Innovation Journal*, *3*, 1–15. https://doi.org/10.18060/25636

Bellagarda, J., & Abu-Mahfouz, A. M. (2022). Connect2NFT: A Web-Based, Blockchain Enabled NFT Application with the Aim of Reducing Fraud and Ensuring Authenticated Social, Non-Human Verified Digital Identity. *Mathematics*, *10*(21), 3934. https://doi.org/10.3390/math10213934

Chalmers, D., Fisch, C., Matthews, R., Quinn, W., & Recker, J. (2022). Beyond the bubble: Will NFTs and digital proof of ownership empower creative industry entrepreneurs? *Journal of Business Venturing Insights*, *17*, e00309. https://doi.org/10.1016/j.jbvi.2022.e00309

Grishchenko, I., Maffei, M., & Schneidewind, C. (2018). A semantic framework for the security analysis of Ethereum smart contracts. In *Lecture Notes in Computer Science* (pp. 243–269). https://doi.org/10.1007/978-3-319-89722-6_10

Gutte, Y., Vora, A., Sharma, Y. K., & Bhardwaj, B. (2022). NFT Marketplace based on Ethereum Blockchain. *International Journal of Advanced Research in Science, Communication and Technology*, 179–186. https://doi.org/10.48175/ijarsct-3729

Kshetri, N. (2022a). Scams, frauds, and crimes in the nonfungible token market. *IEEE Computer*, *55*(4), 60–64. https://doi.org/10.1109/mc.2022.3144763

Kshetri, N. (2022b). Scams, frauds, and crimes in the nonfungible token market. *IEEE Computer*, *55*(4), 60–64. https://doi.org/10.1109/mc.2022.3144763

Liu, X., Muhammad, K., Lloret, J., Chen, Y. W., & Yuan. (2019). Elastic and cost-effective data carrier architecture for smart contract in blockchain. *Future Generation Computer Systems*, *100*, 590–599. https://doi.org/10.1016/j.future.2019.05.042

Nadini, M., Alessandretti, L., Di Giacinto, F., Martino, M., Aiello, L. M., & Baronchelli, A. (2021a). Mapping the NFT revolution: market trends, trade networks, and visual features. *Scientific Reports*, *11*(1). https://doi.org/10.1038/s41598-021-00053-8

Nadini, M., Alessandretti, L., Di Giacinto, F., Martino, M., Aiello, L. M., & Baronchelli, A. (2021b). Mapping the NFT revolution: market trends, trade networks, and visual features. *Scientific Reports*, *11*(1). https://doi.org/10.1038/s41598-021-00053-8

Oates. (2009). A methodology for developing 'Chainlink' converters. *European Conference on Power Electronics and Applications*, 1–10. http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.ieee-000005278738

Pinto-Gutierrez, C., Gaitán, S., Jaramillo, D., & Velasquez, S. (2022). The NFT hype: What draws attention to Non-Fungible Tokens? *Mathematics*, *10*(3), 335. https://doi.org/10.3390/math10030335

Tariq, S. A., & Sifat, I. M. (2022). Suspicious Trading in Nonfungible Tokens (Nfts): Evidence from Wash Trading. *Social Science Research Network*. https://doi.org/10.2139/ssrn.4097642

Von Wachter, V., Jensen, J. R., Regner, F., & Ross, O. (2021). NFT Wash Trading: Quantifying Suspicious Behaviour in NFT markets. *Social Science Research Network*. https://doi.org/10.2139/ssrn.4037143

Wang, Y. (2022). Volatility spillovers across NFTs news attention and financial markets. *International Review of Financial Analysis*, *83*, 102313. https://doi.org/10.1016/j.irfa.2022.102313

White, B. A., Mahanti, A., & Passi, K. (2022). Characterizing the OpenSea NFT marketplace. *Companion Proceedings of the Web Conference 2022*. https://doi.org/10.1145/3487553.3524629

Wu, J., Lin, K., Lin, D., Zheng, Z., Huang, H., & Zheng, Z. (2023). Financial Crimes in Web3-Empowered Metaverse: Taxonomy, countermeasures, and opportunities. *IEEE Open Journal of the Computer Society*, *4*, 37–49. https://doi.org/10.1109/ojcs.2023.3245801

Campo, A. (2021). Blockchain, NFT & Crypto Art Stato dell'arte di una nuova tecnologia, approcci e sviluppi= Blockchain, NFT & Crypto Art State of art of a new technology, approaches and developments (Doctoral dissertation, Politecnico di Torino).

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