WTF are NFTs?!

This work was part of the course:
Shaping a DCent.Society: Societal Implications of Bitcoin, Blockchains & Smart Contracts
by Dr. Marcus M. Dapp, in the Spring Semester 2024 at ETH Zurich

Abstract

This paper provides a detailed examination of Non-Fungible Tokens (NFTs), including their definitions, uses, and the various platforms that make it possible to create and trade them. The analysis aims to compare different NFT platforms and highlight their respective strengths and weaknesses, providing guidance on the best platform for publishing NFTs.

The examination focuses on NFTs in Ethereum and Bitcoin-based crypto arts. Understanding the differences between Ordinals, Stacks, Ethereum-based NFTs, and RBG projects is crucial to understanding these differences.

In addition to this paper, an NFT has been created and published on both Bitcoin and Ethereum platforms. The design was inspired by the course 'Shaping a Decentralised Society'. The methodology for creating and publishing this NFT is thoroughly described, providing a practical perspective to the theoretical discussions presented.

In the end, the paper summarises its findings into practical recommendations, guiding the reader towards the most appropriate platform for the publication of an NFT, based on the comparative analysis carried out. The paper contributes to the academic understanding of NFTs and provides a valuable resource for practitioners navigating the evolving landscape of digital assets.

Contents

1 Introduction

1.1 Definition of Non-Fungible Tokens

A Non-Fungible Token (NFT) is a unique digital identifier that is recorded on a blockchain and is used to certify ownership and authenticity[40]. NFTs can represent digital or real-world items like artwork and real estate[41]. They can be traded and exchanged for money, cryptocurrencies, or other NFTs, depending on the value the market and owners have placed on them[41]. However, the ownership of an NFT as defined by the blockchain has no inherent legal meaning and does not necessarily grant copyright, intellectual property rights, or other legal rights over its associated digital file[40].

1.2 Purpose and Utility of NFTs

NFTs are a solution to a problem that is as old as the web: the endless replicability of digital information online[44]. They provide the ability to securely value, purchase, and exchange digital art using a digital ledger[46]. NFTs aimed to help artists protect their creations by connecting them with sellers and investors directly[45]. They allow artists and content creators to monetize their work[27].

NFTs can also be used in many other ways, including proving that you attended an event, certifying that you completed a course, owning items for games, digital art, tokenizing real-world assets, proving your online identity, gating access to content, and ticketing[42]. They can represent ownership of something unique, such as a particular music clip or video[31]. NFTs can also represent tangible assets, such as real estate, artwork, or automobiles[31]. The NFT has a particular owner, and ownership may be transferred to another via a contract[31]. In this way, NFTs and the assets they represent may be traded on open marketplaces[31].

2 Comparison of NFT Platforms

2.1 OpenSea

OpenSea is a well-known platform in the world of NFTs, offering over 80 million NFTs for buying and selling, including art, collectibles, domain names, music, photography, sports, trading cards, utilities, and virtual worlds. [25] It supports various file formats, including GLB, GLTF, JPG, PNG, GIF, SVG, MP4, WEBM, MP3, WAV and OGG files, which can be uploaded by the user and supports 15 different wallets at the moment. [8]

The platform has a good understanding filtering mechanism to chose from at the top of the page. The current trends can be seen, as well as the current stats. Even for someone who is new in the field, the website is simple structured and all the important information can be easily found. There are eight different languages to choose from, covering the most common ones. The platform provides a clear and concise overview of frequently asked questions and tutorials at the bottom of the page. Additionally, users can easily access information on the website itself, ensuring a deeper understanding of the content.

OpenSea is compatible with 8 different blockchains. Ethereum, Polygon (an EVM-compatible Ethereum sidechain), Klaytn, Arbitrum (which uses Ethereum as its base chain for security), Optimism, Avalanche, The Zora Network (launched in 2023), and Base (also built in 2023) [29].

The platform does not charge any account fees, so creating an account is free for users. However, a fee of 2.5% is charged on the buyer side when purchasing NFTs. [18]. Additionally, creators can earn a 'Creator Fee' called Royalties. Every time an NFT is sold on OpenSea, the seller can set the fee up to 10%, [24]. which is relatively low compared to other platforms like Rarible. [18] OpenSea allows the seller to choose between an auction or a fixed price for the NFT.

It is important to note that cryptocurrency is needed to buy or sell NFTs. OpenSea has recently introduced a new feature that allows Cryptocurrencies to be purchased directly with a credit or debit card via MoonPay. However, this method incurs high fees, so it may be cheaper to buy cryptocurrencies through other means. Even when the user does not have a wallet yet one can simply sign up with an email and create a wallet. The newly created wallet is fully integrated with OpenSea so this is ideally for beginners to start with. [32]

OpenSea's security has been a topic of controversy due to several bugs in the past that resulted in financial losses, as noted by [7]. Instances of stolen artwork have also been reported. In such cases, users can file a ticket, although it should be noted that OpenSea has been known to close these without resolving the issue, as pointed out by [48]. While no platform can be completely free of bugs, it is important to stay informed about them.

2.2 Rarible

Rarible is a well-known platform for NFT traders. It allows for the publication of various types of content, such as art, photography, games, metaverse, music, domains, DeFi, Memes, Punks, and NSFW.

The platform currently supports Ethereum, Polygon, Immutable-X, zkSync Era, and RARI-Chain blockchains. [47]

Rarible offers a user-friendly filter that enables users to search for blockchain sale types and price ranges, making it easy to find specific items. It supports various file formats, including PNG, GIF, WEBP, MP4, and MP3, and is compatible with ten different wallets. [8]

The platform has a simple structure and displays the latest drops and trending NFTs. However, it lacks a FAQ section, which may cause confusion for total beginners. Additionally, it only supports English, which may make it difficult for non-native speakers to use. Notably, the website includes a bug bounty link at the bottom of the page to encourage users to report bugs and receive rewards. This indicates that the developers are aware that bugs and errors can happen, but wants to encourage ethical hacking.

Rarible does not charge an account fee, but it does charge a 2.5% fee to both buyers and sellers. Sellers have the option to set royalties up to 30% to increase their profits. [8] One advantage of Rarible is the ability to split royalties among collaborators. This feature allows for easy income distribution within a team.

The security of Rarible is technically sound, but as with any system, there are always new threats to overcome. In April 2022, Checkpoint published an article highlighting a security flaw in Rarible that could have led to stolen NFTs. [6]

Users can anonymously buy and sell NFTs. While anonymity is important in the crypto world, it can also pose risks as other users may not be verified and could potentially launder money. [17]

Rarible allows users to pay with cryptocurrencies as well as credit cards. However, like other NFT platforms, a crypto wallet is required to buy or sell NFTs. Credit card fees range from 2.5% to 4% and are relatively high. [17]

2.3 Diba

Diba, the first platform that exchanges Bitcoin-based NFTs, was officially launched on the mainnet on May 18th, 2023[16]. The marketplace allow users to trade any asset with Bitcoin smart contracts protocol on layer-2 networks, such as Lightning Network. The NFTs will be hosted on high availability storage and cloud services provided by Hut 8[36], a publicly traded bitcoin miner in North America. DIBA also released a Bitcoin-only wallet in partnership with HUT. [16]

Diba uses RGB (Really Good for Bitcoin) smart contract protocol to exchange NFTs[34]. Gideon Nweze, DIBA's co-founder, argues that the RGB protocol provides more cost-effective and private transactions, a much-needed feature considering the increasing Bitcoin network transaction fees[15]. This is because NFTs inheriting all of the same qualities of Bitcoin means lower fees and security backed by the strongest blockchain. This is an entirely new structure than what the Bitcoin and digital art communities have seen before. [34]

In 2023, during the Bitcoin Miami conference, Diba organized a curated drops event, which invites one performance artist (OONA) and four digital artists (Bradley Hart, Lil Bitcoin, MEAR ONE, Krista Kim). The purpose was to amplify Diba's presence within the community, following its recent official launch on the mainnet. [11]

Currently, there are a total of 21,042 items available for sale on Diba. When sorted by status, there are no items listed as "has offer" or "on auction", suggesting limited trading activity. All items fall into either the "buy now" or "new" categories, with 21,042 items in each.

When sorted by price, the majority of items are priced at 0, with a few priced at a couple of satoshis (equivalent to less than 1 USD cent). A small number of items are priced higher, reaching several tens of US dollars, but their content is currently not visible and marked as "coming soon", indicating potential future exhibition. The affordably priced items are named with human-readable phrases like "freedom for humanity", while the pricier "coming soon" items are identified by alphanumeric strings such as "684af08c-3431-4f", likely serving as exhibit identifiers for future events.

With the implementation of smart contract protocols, BitMask is the first and only noncustodial wallet to support stablecoins and NFTs, allowing for better privacy and security for digital assets using the Bitcoin blockchain. In order to create, trade, and collect on the DIBA marketplace, the user needs to connect to BitMask and fund their Vault. [12]

2.4 Binance

Binance is a global cryptocurrency exchange that has been providing trading services for over 150 cryptocurrencies since its establishment in 2017, including Bitcoin, Ethereum, Litecoin, and its own BNB token. Since early 2018, Binance has been the world's largest cryptocurrency exchange by trading volume. Founded in China, Binance relocated its servers and headquarters to Japan in September 2017 following a Chinese government directive banning cryptocurrency trading. [28]

The Binance NFT marketplace is a marketplace that features all forms of digital artworks and collectibles. Powered by the Binance blockchain infrastructure and community, the Binance NFT marketplace provides a high liquidity platform for users to launch and trade NFTs. [5]

The platform features 3 product lines[5]:

- *Marketplace*: Mint, sell, bid, and buy NFTs from creators around the world.
- *Events*: Buy exclusive NFTs created by global artists and influential brands. Enjoy premium offerings from digital artists, musicians, athletes, and celebrities.
- *Mystery Boxes*: Boxes that contain one random NFT in 4 rarity levels: normal, rare, SR, SSR.

Only verified users with at least 10 followers on Binance NFT can create NFTs on Binance.[2] Binance also requires users to complete identity verification(i.e. uploading ID document, live detection) before accessing its products and services, including deposits, trading, and withdrawals. Unverified accounts are limited to services such as withdrawals, order cancellations, closing positions, and redemptions.[1]

In response to user concerns regarding security, the Binance website assures that the verification is taken to ensure the account safety and to prevent users from being subjected to fraud, engaging in corruption, money laundering, or financing terrorism. Additionally, the uploaded documents are treated with the utmost confidentiality. [3]

Binance currently accepts the following file formats for upload: image(jpeg, png, gif), video(mp4, mpeg, avi), and audio(wav, mp3). The maximum file size is 50MB. [2]

The transaction fee on Binance[4] includes the following parts:

- *Platform fee*: When you sell an NFT on Binance NFT, a flat 1% platform service fee on the sale price will incur.

- *Royalty fee*: very time an NFT is sold, a percentage of the sale price (royalty fees) will be paid to compensate the original NFT creator. Sellers need to pay a royalty fee (0-10%) to the creator, according to the royalty fee the NFT collection creator set.
- *Deposit fee*: Depositing an NFT to Binance NFT Marketplace will incur a gas fee, which goes to the miners responsible for processing the transactions. The gas prices fluctutate according to network traffic.
- *Withdrawal fee*: Withdrawals to crypto addresses outside of Binance NFT typically incur a transaction fee, which goes to miners responsible for processing the transactions.

3 Design of NFT

We have designed an NFT that represents the lecture on 'Shaping a Decentralized Society' in some parts. The goal was to encourage critical thinking about today's world and raise awareness. The image is rather dystopian and is created in pixel art, with a childish aspect that makes the dystopian scenario more grotesque.

The world is shown in the centre of the picture. half of it brown and the other half green. The two different colours should represent the decline of the world and its gradual downfall. The majority of people's goal is to gain money, which makes them emotionally dead. The two skeletons in the passage also represent this idea. Capitalism is responsible for killing people, not only physically but also mentally. The whole world is on fire, but no one seems to care or has no feeling of responsibility to have the desire to change it.

In the bottom left corner, there is a representation of a skeleton sitting on a chair. Although it is meant to represent nobility, wealth, and success, it ultimately does not change the outcome.

In the bottom right corner, there is a radio clock displaying the time as 11:55. This serves as a symbol to remind people that it is time to change their lifestyle. Additionally, there is an image of a hand grasping bitcoin, which may prompt questions such as 'What brings happiness?' and 'What do I want to remember when I am old?' In the final moments of this person's life, their thoughts were about money and material possessions.

It is important to note that there are positive aspects to both capitalism and bitcoins.

The left side of the image is bright, and a cloud rains 0s and 1s, which form the foundation of the entire currency. The image depicts the creation of new things and the cleanliness of electronic coins. These binary digits are translated to ASCII, which spells out the word 'HOPE.'

On the right-hand side, there are graphs in purple, yellow, and red, depicting the fluctuating trends of cryptocurrencies over time.

The skeleton on the right is holding half a bitcoin, symbolising the halving that occurred in April of this year.

Figure 1: Dystopian NFT

4 Creating Non-Fungible Tokens

4.1 Bitcoin Ordinals vs. Ethereum NFTs

Bitcoin and Ethereum have similarities and differences in their approach to creating and designing crypto art. The main difference between ordinals and NFTs is how they are stored. Traditional standards for NFT usually only contain metadata or a URL pointer to some off-chain data and permit owners to modify or update the visuals of some NFTs. Ordinals, however, store the content on the blockchain via inscriptions and are therefore fixed. The intention here is to make ordinals more decentralised and resistant to censorship. But it also makes them more expensive and limited in size. [22] [37]

Storing the entirety of the NFT on the blockchain leads to two main issues: increased blockchain size and higher inscription costs. This increase in size will require all nodes to store more data for an already 500GB+ blockchain and can potentially be problematic for low-cost setups that only have 1 or 2 hard drives. If these nodes drop out from the network, Bitcoin will gradually become less decentralized, increasingly dominated by entities capable of handling the growing storage demands. Furthermore, inscription costs, especially for images and audio, will inevitably start out significantly higher than those of Ethereum approaches, as miners will be tasked with handling larger streams of data.

Ordinals are bigger in size since they store all the data and content on the satoshi. A satoshi is the smallest discrete unit of the cryptocurrency Bitcoin (BTC), named after Bitcoin's founder, Satoshi Nakamoto. [21]

Ordinals, as of right now at least, do not offer any notably complex functionalities that already exist in Ethereum. Ethereum allows for the creation of programmable, interactive NFTs that can engage in self-executing contracts and royalties, features that are widely used in NFT collections and projects. This limits much of the headroom for Ordinals to evolve, considering that Ethereum also started supporting more common programming languages, allowing developers to jump right in without any significant hurdles, a flexibility that cannot be said about Bitcoin's archaic programming language. Regardless, Ordinals are relatively new and, given the unpredictability of the crypto space, no one could really make accurate presumptions about their viability or success, considering that their unique approach to storing data can reduce the possible attack vectors present in Ethereum's implementation.

NFTs store all the heavy data off-chain. Another difference is that Bitcoin ordinals can be used as an ordinary Bitcoin. As an example, a Bitcoin user that does not care about an ordinal it has, then it can be used like an ordinary Bitcoin. It is fungible. [14]

Another difference is how they are added to their respective blockchain networks. Minting Ordinals contributes to the already massive Bitcoin network energy requirements. NFTs on chains consumes much less energy and are faster. [41]

Here is a summary for the differences in Ethereum NFTs and Ordinals [35] [37] [23]:

Features	Bitcoin Ordinals	Ethereum NFTs
Data storage	Stored on Bitcoin Blockchain	Stored on decentralized apps through self-executing smart contracts
Immutability	Highly immutable	Data can be updated
Rarity and value	Ordinal position and content	Token standard, community perception
Smart contracts	None	Leveraged for complex functionality
Transaction fees	Higher: on-chain storage	Lower: off-chain storage
Fungibility	Both fungible and nonfungible	Predominantly nonfungible
Compatibility	certain blockchain technologies or platforms	Widely supported across various blockchain platforms

Table 1: Differences between Ordinals and NFTs

4.2 Ordinals

Ordinals represent a relatively new feature of Bitcoin's functionality, to facilitate the prevalence of NFTs directly inscribed on the Blockchain. Unlike the implementations of NFTs in Ethereum, where the data is stored externally and only referenced from the Ethereum blockchain through the use of Smart Contracts, Ordinals inscribe data directly

onto Bitcoins. Namely, each Bitcoin consists of 100 million Satoshis (or sats), with one Satoshi being the smallest division of a Bitcoin. Each Satoshi is unique and can be traced back to its creation, by having it assigned with a number based on its minting order. As of January 20, 2023, this numbering system has allowed for inscribing data to a specific Satoshi, making it possible to inscribe Images, Audio, Video or Text on the Bitcoin Blockchain. [10]

Each Transaction's structure is inputs and outputs, whereby the information on that Transaction is recorded inside a component known as the "witness." A soft fork was implemented via a protocol called Segregated Witness (SegWit) [20] that modified how transaction data is stored, namely separating signature information(witness) from the transaction data. This separation opened up the possibility to embed arbitrary data, such as images, audio or text, directly in the witness part of transactions.

Ordinals then used this feature to inscribe data into the witness. As described in the section above, ordinal numbers took this feature and made use of it as a means of storing data in the witness. This method allows for the embedding of the data into a given Satoshi; hence, this data is associated with its transactional history and becomes unique and traceable.

With scripts, a standard Bitcoin transaction can be executed with the NFT's data presented into a new output. These scripts are visible and verifiable by all network participants, thus making the process transparent and immutable. The so-called taproot upgrade that soon followed supplemented SegWit by introducing Schnorr [19] signatures and drastically improving the process. These signatures further optimize multi-signature transactions, which are typical in NFT transactions, whereby they look like single-signature, thus increasing privacy and data efficiency for the blockchain. [39]

4.3 Stack

There are two main methods on how to create an NFT. The stack method is a more straightforward method . The stack allows a large number of people to create and trade NFTs because of its simplicit:.This method involves the token being connected indirectly through a smart contract to a blockchain, rather than being directly inscribed in the blockchain. This is the most popular method for creating NFTs as it is cheaper. This may appear less secure than a blockchain-linked digital object, but the use of smart contracts offers a high level of protection. Smart contracts are simply contracts whose conditions are inscribed in the blockchain and are automatically executed as soon as the contract terms are met. This ensures that the conditions of the contract cannot be altered by anyone. As soon as the smart contract is published nobody can change it anymore, therefore the security of our token which is linked through a smart contract is also guaranteed by the blockchain. It is cheaper (you will need less space on the blockchain) to create a smart contract than to inscribe our object directly to the blockchain. To recap, the stack method allows the user to link a digital object to the blockchain, which is usually Ethereum, through a smart contract which will guarantee its security and tradability. This mechanism is called a Proof of Transfer. [37] Ethereum is usually used because it is the most popular cryptocurrency for NFTs. [30] Although Bitcoin and Ethereum are now used equally, this is due to the popularity of Bitcoin ordinals, which are widely used for the creation of Stack-based NFTs. Ethereum, however, has been the preferred cryptocurrency for the creation of blockchain-based smart contracts and it almost monopolised the NFT marketplace before the emergence of Bitcoin based ordinals.

4.4 RGB Project

RGB Smart Contract Protocol, previously called BHB Network, was developed by Giacomo Zucco and first launched in 2016. It uses the Lightning Network functionality and enables users to mint NFTs without using much space on the Bitcoin network. It operates like a layer-2 ecosystem since it manages the data of the smart contract and the code off-chain. [13]

The two main advantages of using the RGB protocol to mint NFTs are: higher scalability, and lower transaction fees.[13] Regarding scalability, since the smart contract remains outside the blockchain, the limited space of the blockchain does not affect the performance of RGB protocol. Therefore, the RGB has all the parameters to scale in terms of network size, data size and throughput. Regarding transaction fees, the transaction fees on the RGB protocol are very low since the activities such as minting NFTs are done off-chain. As a result, it reduces congestion on the Bitcoin blockchain.

The primary NFT platform that currently supports the RGB protocol is Diba (Digital Bitcoin Art and Asset)[34]. It is also the first platform to utilize RGB for NFTs.

4.5 Publish NFT on Bitcoin Platform

4.5.1 Process Overview

When it comes to actually inscribing sats, there are two viable options: doing it locally, or using OrdinalsWallet. From those two options, the safest one will always be to do it locally, but it requires time and knowledge, whereas the latter proves to be more user- and beginner-friendly. That aside, when operating under a true zero-trust mindset, where one should not put trust in third parties with their assets, the "correct" option is to be in control and do it oneself. However, it is important to acknowledge the effort certain individuals have put into making Ordinals widely accessible, generating more traction for an already promising platform.

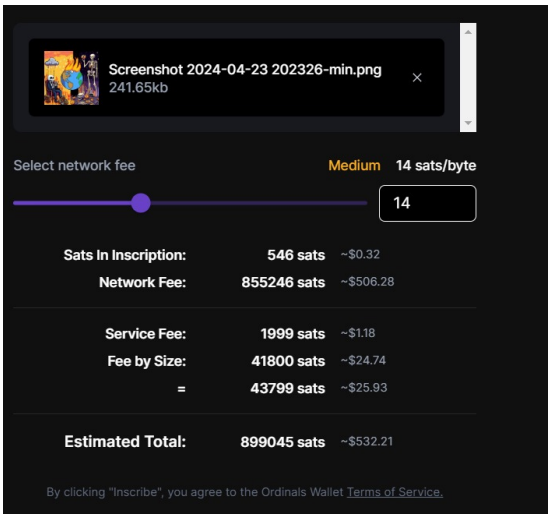

Figure 2: Inscription Costs

This process requires a full Bitcoin node, the software wallet "Bitcoin Core," an open-source library called "Ord," [43]and, of course, funding. Due to the bitcoin halving and other factors, the cost of inscribing Ordinals has dramatically increased to the point, that it would be unrealistic to inscribe anything larger than a few lines of text at the moment. However, the process is demonstrated using the regtest environment, which operates identically to the mainnet.

```
C:\Users\theod\Downloads\ord-0.17.1-x86_64-pc-windows-msvc\ord-0.17.1>ord -r env
Index file `C:\Users\theod\Downloads\ord-0.17.1-x86_64-pc-windows-msvc\ord-0.17.1\env\regtest\index.redb` needs recovery
. This can take a long time, especially for the --index-sats index.
Listening on http://0.0.0.0:9001
`ord` server URL:
http://127.0.0.1:9001
Example `bitcoin-cli` command:
bitcoin-cli -datadir=env getblockchaininfo
Example `ord` command:
C:\Users\theod\Downloads\ord-0.17.1-x86_64-pc-windows-msvc\ord-0.17.1\ord.exe --datadir env wallet balance
```

Figure 3: Starting the Environment

After syncing the entire blockchain, which exceeds 500 GB, the user becomes an active network participant (node). It's important to note that pruned nodes, which store only part of the blockchain, will not suffice because the origin needs to be traced and positioned for every single Satoshi. Utilizing the open-source library "Ord" on Github [43], transactions can be submitted after setting up the local environment. The ord library establishes a connection to Bitcoin Core via the Remote Procedure Call (RPC) protocol, a common protocol for sending instructions to a computer over the internet, thereby enabling the user to create a wallet that supports inscriptions, as Bitcoin Core does not natively support this functionality. To begin the inscription process, the wallet needs to be funded by sending Bitcoins to this address. The transaction will not be visible or actualized on the blockchain immediately; a few blocks must be mined first in order to appear on explorers. The waiting time can vary greatly, since a transaction is first submitted to the Memory Pool (mempool) and, from there the transactions with the highest fee rates are prioritized. Setting them too low could mean that the transaction will never be processed.

```
C:\Users\theod\Downloads\ord-0.17.1-x86_64-pc-windows-msvc\ord-0.17.1>ord.exe --datadir env wallet receive
{
  "addresses": [
    "bcrt1pj3yhntgz2ccg6gsfqt8c3pl366s0aecp72mh87fgz4mkps52nmzq07wqw8"
  ]
}
```

Figure 4: Generate Funding Address

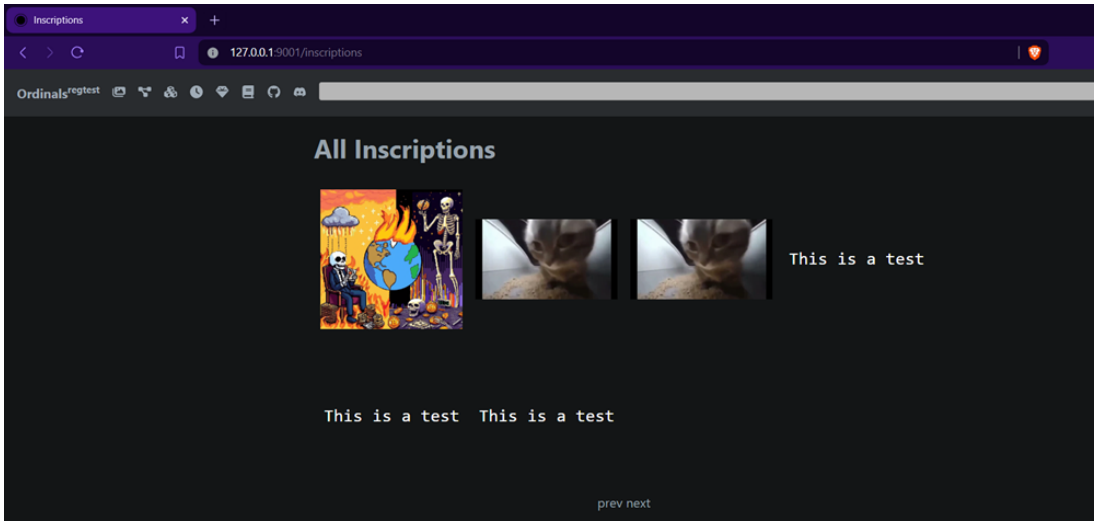

Figure 6: Ordinals Interface

```
C:\Users\theod\Downloads\ord-0.17.1-x86_64-pc-windows-msvc\ord-0.17.1>ord.exe --datadir env wallet inscribe --fee-rate 5000 --file wtf.png
{
  "commit": "4dbf9732b3c69a8577d81bece3adf60230d1acdb79eff36d5dcb9b6c400e54f7",
  "commit_psbt": null,
  "inscriptions": [
    {
      "destination": "bcrt1p0q8mfpnn5nadhgjzxfwglawttgeqk9eyu7tvcyh2hrjh2q6h4e0skmmflv",
      "id": "6f9ed8cd5076ce3812f037fa207f7fc188346a1ef0b508067fc7c1f2315675aei0",
      "location": "6f9ed8cd5076ce3812f037fa207f7fc188346a1ef0b508067fc7c1f2315675ae:0:0"
    }
  ],
  "parent": null,
  "reveal": "6f9ed8cd5076ce3812f037fa207f7fc188346a1ef0b508067fc7c1f2315675ae",
  "reveal_broadcast": true,
  "reveal_psbt": null,
  "rune": null,
  "total_fees": 305245000
}
```

Figure 5: Inscription Process

After a few blocks, the inscription will be registered on the blockchain and visible on explorers like Ordinals. However, since this is done for demonstration purposes, the inscribed NFT will not appear on the main net but will be visible to a local host. Minting through OrdinalsWallet: As previously stated, this is the most common method for minting NFTs on Bitcoin, requiring only the funds for the inscription and a supported browser wallet. This process is time-efficient and hassle-free, but it does involve a potential security compromise by trusting a third party with the user's funds. The trade-off, however, is not significant because the transaction needs to be signed off with the user's password by these open-source browser wallets. It is worth noting that using a website is not always necessary for signing transactions, as this can be done using a local express server through APIs provided by most wallets. An example can be found in the Xverse wallet documentation [38] where with minimal knowledge you can mint NFTs yourself without needing to use sites.

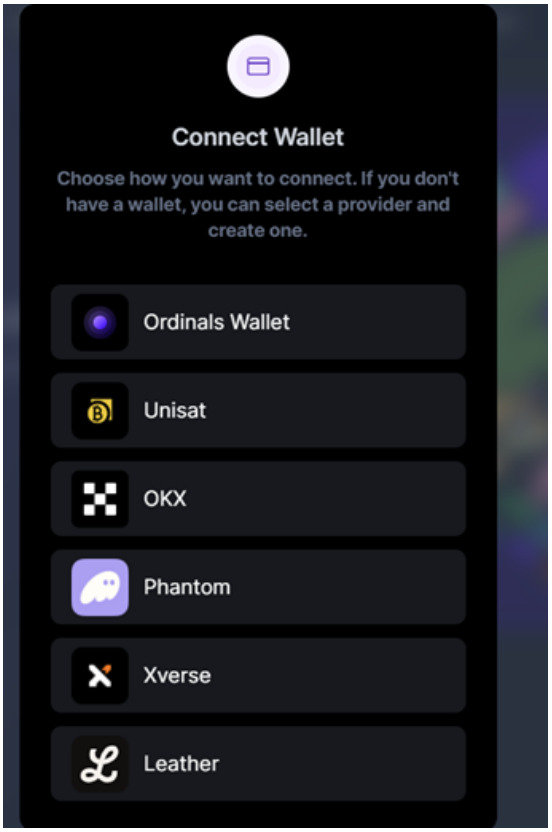

Figure 7: Select Wallet

This, however, only provides a middle ground between complete self-sufficiency and relying on a third-party provider. Both options, using a browser wallet and third-party websites, employ their nodes for verification and minting purposes and should ideally be avoided if maximum security is a concern.

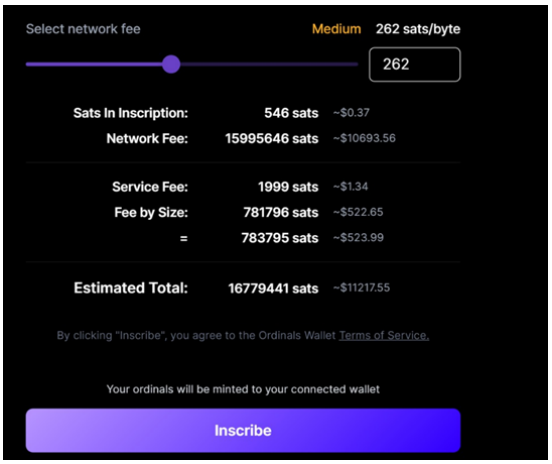

Figure 8: Inscription Process

4.5.2 Technical Considerations and Costs

While Ordinals seem promising, some significant drawbacks and limitations still inhibit their widespread adoption. Bitcoin was meant to represent a store of value, rather than a financial asset. It is designed as the bare minimum basic implementation of a working currency that is anonymous and decentralized. In 2008, no one would have thought that decentralised technologies would lead to Web3, allowing for storing other digital assets aside from currencies. Bitcoin had no programming language to employ smart functionalities in the way transactions were made, whereas Ethereum

was by design capable of it. Bitcoin's native language, Scripts, was made for optimizing transaction efficiency and security, while Ethereum's Solidity, on the other hand, could create complex Decentralized Apps (DApps) like self-executing contracts and Decentralized Finance (DeFi) applications, like self-regulating Crypto Exchanges. From a technical standpoint, ordinals were an afterthought rather than a native feature, making them harder to work with, something that is reflected in the higher prices for minting that one must pay to the miners.

This, however, leads to the following argument: as block rewards continue to halve, the economic incentives for miners need to be accounted for accordingly. Ordinals can subsidize the reduction in block rewards by incorporating fees for minting NFTs, which could be beneficial for ensuring the long-term functionality of the blockchain. With every block halving the miner rewards are also cut by half, an example being the halving that happened on April 2024, where the rewards for every block mined went from 6.25 BTC to 3.125 BTC. It is estimated that by 2140, all 21 million Bitcoins will have been mined, leaving miners with no rewards for completing new blocks. [9] This, in itself, poses a huge risk for the network's survival, and unless new features are added. Ordinals appear to be the most viable option for sustaining it.

Judging from the past, nothing can really be said about the future of ordinals. Almost all crypto projects and innovations fail, but there are a few that offer enough utility to the broader public that prevail. The unique approach of Ordinals to NFTs seems promising enough to ensure their longevity and utility. Bitcoin, being the most traded, widely recognized, and extensively used cryptocurrency, inherently offers a solid foundation for a sustainable alternative to Ethereum NFTs. Given that Ordinals inscribe data directly onto the blockchain, this integration promotes a more secure environment, allowing for future growth. This strategic positioning could very well secure their place as a pivotal development in the blockchain space.

4.6 Publish NFT on OpenSea

4.6.1 Process Overview

In order to publish an NFT using the stack method it must firstly be considered which platform to use. There are many different platforms but at the end of the day, the process of publishing stays the same. Firstly, an account needs to be created on the platform and a crypto wallet must be obtained. There are many ways to create a cryptocurrency wallet, but it can be easily done on any platform chosen for publishing your NFT. Afterwards, it is necessary to purchase cryptocurrency that is supported by the platform (Ethereum is the most popular). There are numerous types of wallets, but it is usually not complicated to link them to another platform in case the user already has a wallet and wishes to link it to the NFT publishing platform. Following this, a collection must be created in which the user will store their NFT. This step will cost the user some cryptocurrency. After this, the user is able to create their own NFT within the collection and publish it on the platform's market. The creation of the NFT will also require the user to pay a fee in cryptocurrency. The creation of the NFT should look like the following figure, with the price being the amount the user wishes for it to be sold for.

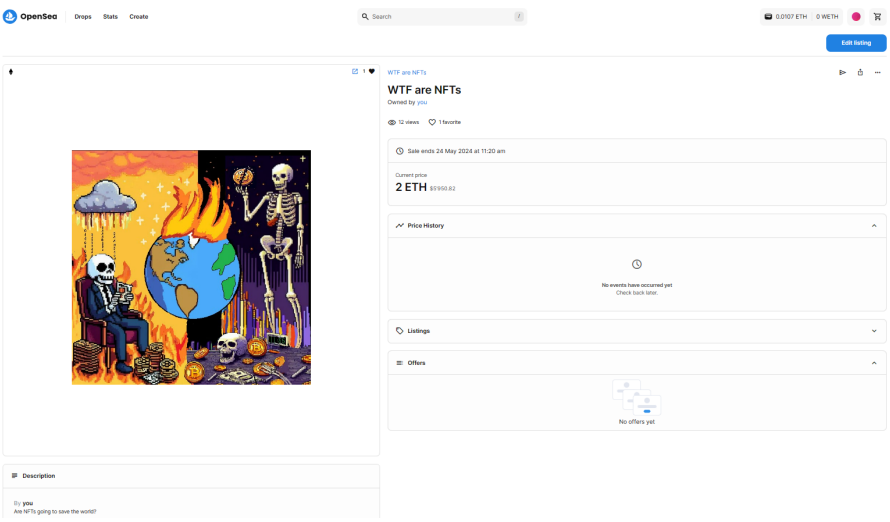

Figure 9: Published NFT

The NFT was created using the OpenSea platform, which is very user-friendly and offers a convenient interface. For those interested in creating and trading NFTs, OpenSea is an excellent choice. Similarly, there are other platforms

that offer similar functionality, such as GAMMA. While there are minor differences in the types of cryptocurrency wallets accepted and the platform fees for creation, these platforms are generally comparable. For us, OpenSea was chosen because it seemed more user-friendly but any such platform could have been used and would have gotten us the same result. OpenSea is also by far the most popular platform for a NFT marketplace. [33]. It always had at least 60% market share of the whole NFT marketplace. Therefore it made more sense to use OpenSea than GAMMA for example.

4.6.2 Technical Considerations and Costs

From a technical standpoint, the process is relatively straightforward. The platforms do provide a certain degree of ease of use, but it is still necessary to read all instructions carefully, as there may be important steps that are overlooked. It is also necessary to verify that your digital object is compatible with the platform. On OpenSea, the file format can be JPG, PNG, GIF, SVG, or MP4, and the file size must be less than 50 MB. It is possible that certain issues may arise depending on the platforms in question. For instance, when our NFT was published as a JPG, the image failed to appear, accompanied by a message indicating that it could not be loaded. The Figure below illustrates this situation: In order to correct the issue, the metadata of the NFT had to be updated. This can be done

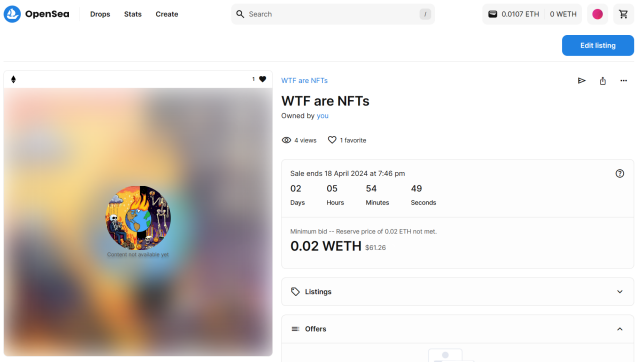

Figure 10: Content not available

easily by clicking on the three dots in the top right corner and selecting "refresh metadata." Otherwise, there were no other problems or complex technical considerations. The exact reason for this error is unknown, but it is common on OpenSea and can be easily corrected. This problem is encountered by many people, and there are numerous forums where people address it. It is possible that phishing emails may be received when an NFT is published and listed for sale. Our group has received several emails stating that our item was sold and offering the option to cash out our funds. However, these emails imitate the interface of OpenSea and attempt to mislead the recipient into believing that they are actually from OpenSea. It is therefore advisable to be extra careful when emails from OpenSea are received and to double-check the address of the mail. The process of NFT creation is costly because it requires the use of smart contracts, which consume space on the blockchain. This in turn requires the expenditure of cryptocurrency. For the NFT of this course, the total cost was approximately 0.02 ETH, with the platform fees adding up to approximately 60 CHF. We then attempted to sell it at a similar price, but it did not sell. It is now listed again for 2 ETH, with no expectation of a sale. [26]

5 Recommendation for Selling a JPG

When it comes to creating, selling, and trading NFTs, there are several options available. One must first decide which inscription technology to use: Stack or Ordinals. From a practical standpoint, it is much easier and cheaper to use Stack technology. The added security provided by Ordinal technology is often not worth the additional resources required to create Ordinals. The smart contracts underlying Stack NFTs offer robust security, making Stack technology the more straightforward and cost-effective choice. It requires less computational power and fewer blockchain resources, reducing financial costs.

The popularity of Stack technology has led to the development of numerous user-friendly platforms, with OpenSea being a prime example. OpenSea offers a highly intuitive interface and is one of the largest and most well-known NFT marketplaces. Its high activity level increases the probability of finding buyers and provides a robust support network for NFT sellers. As a market leader, OpenSea invests heavily in security measures and supports multiple blockchains, including Ethereum and Polygon. This flexibility allows users to choose blockchains based on cost or speed considerations.

OpenSea accommodates a wide range of digital assets, including JPGs, MP4s, GIFs, and more, allowing creators to publish a diverse array of content. This feature appeals to both novice and advanced traders, as it removes limitations on the type of art that can be sold. Creating an account on OpenSea is free, removing financial barriers to entry. The NFT creation process is clearly and comprehensively described, and the steps for publishing and selling are straightforward.

Additionally, OpenSea offers an integrated wallet, enabling users to purchase cryptocurrencies directly with a debit or credit card. This feature simplifies the NFT publishing process, especially for beginners. For these reasons, we recommend OpenSea as the optimal choice for those wishing to explore the world of NFTs. Its user-friendly platform, extensive security measures, and support for multiple blockchains make it an ideal starting point for NFT creators and traders.

6 Conclusion

This paper has explored various sides of non-fungible tokens (NFTs). It delved into the technical foundations of NFTs, compared different platforms, and demonstrated the practical application of publishing an NFT. Specifically, the study examined the development of NFTs on two blockchain systems: Bitcoin and Ethereum, analysing the advantages, disadvantages, innovations, and challenges associated with each system.

The detailed comparisons between leading NFT platforms, including OpenSea, Rarible, Diba, and Binance, highlighted the strengths and weaknesses of each, providing valuable insights for users in selecting a suitable platform. The practical section of designing and publishing an NFT bridged the gap between theoretical understanding and real-world application, showcasing the challenges that were overcome. Based on these insights, the paper offers a recommendation for new users on the most suitable platform and explains the reasons behind this advice.

Additionally, the paper provides a comprehensive guideline on Ordinals, detailing their implementation on the Bitcoin Blockchain and contrasting them with Ethereum's NFTs. This comparison is crucial for understanding the unique attributes and potential of each blockchain system for NFT development.

As the cryptocurrency landscape continues to evolve, this paper offers an insightful overview of the fundamental aspects of NFTs, aiding readers in navigating this dynamic field.

References

[1] Binance. *How to complete identity verification on Binance*. https://www.binance.com/en/support/faq/how-to-complete-identity-verification-for-a-personal-account-360027287111. [Accessed: 05.05.2024]. 2019.

[2] Binance. *Binance-Creation*. https://www.binance.com/en/support/faq/how-to-create-your-nft-on-binance-nft-marketplace-79dab23c7d724a069cb90dd709ecd243. [Accessed: 05.05.2024]. 2021.

[3] Binance. *Binance-FAQ*. https://www.binance.com/en/support/faq/how-to-get-started-with-binance-nft-marketplace-2c744531c1fe4bca94936682b91aefb3. [Accessed: 05.05.2024]. 2021.

[4] Binance. *Binance-Fee*. https://www.binance.com/en/support/faq/what-are-the-nft-transaction-fees-on-binance-b0a16587e5394ce9b994d336a38dfb7f. [Accessed: 05.05.2024]. 2021.

[5] Binance. *Introducing Binance NFT Marketplace*. https://www.binance.com/en/support/faq/introducing-binance-nft-marketplace-f2d24d2faf1c4c878acf40df5481086f. [Accessed: 05.05.2024]. 2021.

[6] *Check Point Research detects Vulnerability in the Rarible NFT Marketplace, Preventing Risk of Account Takeover and Cryptocurrency Theft*. https://research.checkpoint.com/2022/check-point-research-detects-vulnerability-in-the-rarible-nft-marketplace-preventing-risk-of-account-take-over-and-cryptocurrency-theft/. [Accessed: 22.04.2024]. 2022.

[7] Yash Gupta, Jayanth Kumar, and Dr. Andrew Reifers. *Identifying Security Risks in NFT Platforms*. 2022. arXiv: 2204.01487 [cs.CY].

[8] *NFT Marketplaces Compared: OpenSea Vs. Rarible*. https://dexterlab.com/nft-marketplaces-compared-opensea-vs-rarible/. [Accessed: 22.04.2024]. 2022.

[9] Bitbo. *Bitcoin Halving Countdown*. https://bitbo.io/halving/. [Accessed: 15.05.2024]. 2023.

[10] Creator of Ordinals Casey Rodarmor. *Inscribing on Mainnet*. https://rodarmor.com/blog/inscribing-mainnet/. [Accessed: 15.05.2024]. 2023.

[11] DIBA. *2023 Bitcoin Conference Drop*. https://diba.io/drop/DIBA_0/. [Accessed: 05.05.2024]. 2023.

[12] DIBA. *CONNECT BITMASK WALLET*. https://diba.io/connect/. [Accessed: 05.05.2024]. 2023.

[13] GateIO. *RGB Protocol Introduces Alternative Bitcoin NFTs with Ordinal Issuance*. https://www.gate.io/fr/blog_detail/2748. [Accessed: 15.05.2024]. 2023.

[14] *How Are Bitcoin Ordinals Different from NFTs?* https://chain.link/education-hub/ordinals-bitcoin-nfts. [Accessed: 22.04.2024]. 2023.

[15] Gile K. *New Non-Fungible Token (NFT) Marketplace DIBA Goes Live*. https://www.bitdegree.org/crypto/news/new-non-fungible-token-nft-marketplace-diba-goes-live. [Accessed: 05.05.2024]. 2023.

[16] Shaurya Malwa. *NFT Marketplace DIBA Goes Live on 'Really Good for Bitcoin' Smart Contracts*. https://www.coindesk.com/tech/2023/05/19/nft-marketplace-diba-goes-live-on-really-good-for-bitcoin-smart-contracts/. [Accessed: 05.05.2024]. 2023.

[17] Emma Newbery. *Rarible NFT Marketplace Review: Flexible and Accessible NFT Platform*. https://www.fool.com/the-ascent/cryptocurrency/nfts/rarible-nft-marketplace-review/. [Accessed: 22.04.2024]. 2023.

[18] Tessa Campbell Rickie Houston. *OpenSea Review*. https://www.businessinsider.com/personal-finance/opensea-review?op=1. [Accessed: 08.04.2024]. 2023.

[19] *Schnorr Signature*. https://en.wikipedia.org/wiki/Schnorr_signature. [Accessed: 15.05.2024]. 2023.

[20] *Segregated Witness*. https://en.wikipedia.org/wiki/SegWit. [Accessed: 15.05.2024]. 2023.

[21] The Investopedia Team. https://www.investopedia.com/terms/s/satoshi.asp. [Accessed: 22.04.2024]. 2023.

[22] Kyle Torpey. *Bitcoin Ordinal NFT: Everything Need to Know*. https://www.investopedia.com/what-are-bitcoin-ordinals-7486436. [Accessed: 05.05.2024]. 2023.

[23] *What Are Ordinals? Bitcoin NFTs Explained*. https://chain.link/education-hub/ordinals-bitcoin-nfts. [Accessed: 05.05.2024]. 2023.

[24] C.-H. Wu, C.-Y. Liu, and T.-S. Weng. "Critical Factors and Trends in NFT Technology Innovations". In: *Sustainability* 15 (2023), p. 7573. DOI: 10.3390/su15097573. URL: https://doi.org/10.3390/su15097573.

[25] OpenSea - About. https://opensea.io/about. [Accessed: 08.04.2024]. 2024.

[26] *Asset on OpenSea*. https://opensea.io/assets/ethereum/0x161c5842e277683b46adc311deeb1e18832dd1d0/1. [Accessed: 19.05.2024]. 2024.

[27] BBC. *What are NFTs and why are some worth millions?* https://www.bbc.com/news/technology-56371912 [Accessed: (2024.3.20)]. 2024.

[28] Binance. *Binance-Wiki*. https://en.wikipedia.org/wiki/Binance. [Accessed: 05.05.2024]. 2024.

[29] OpenSea - Compatible Blockchains. https://opensea.io/learn/blockchain/blockchains-compatible-with-opensea. [Accessed: 08.04.2024]. 2024.

[30] Nicholas Boey. *Top NFT Blockchain By Market Share and Tradings Volume*. https://www.coingecko.com/research/publications/market-share-nft-blockchains. [Accessed: 15.05.2024]. 2024.

[31] CoinDesk. *What Are NFTs and How Do They Work?* https://www.coindesk.com/learn/what-are-nfts-and-how-do-they-work/ [Accessed: (2024.3.20)]. 2024.

[32] OpsenSea Crew. *OpenSea introduces wallet creation using email, making NFT onboarding easier*. https://opensea.io/blog/articles/opensea-new-onboarding-experience. [Accessed: 05.05.2024]. 2024.

[33] Ch Daniel. *OpenSea Revenue and Growth*. https://www.usesignhouse.com/blog/opensea-stats. [Accessed: 15.05.2024]. 2024.

[34] DIBA. *DIBA*. https://diba.io/about/. [Accessed: 05.05.2024]. 2024.

[35] Cem Dilmegani. *Top 5 Differences Between Ordinal Inscriptions vs NFTs in 2024*. https://research.aimultiple.com/ordinal-inscriptions-vs-nfts/. [Accessed: 05.05.2024]. 2024.

[36] HUT-8. *HUT-8*. https://bitcoinmagazine.com/tags/hut-8. [Accessed: 05.05.2024]. 2024.

[37] Guneet Kaur. *Bitcoin Ordinals vs. Ethereum NFTs: A comparative overview*. https://cointelegraph.com/learn/bitcoin-ordinals-vs-ethereum-nfts. [Accessed: 22.04.2024]. 2024.

[38] Secret Key Labs. *Sats Connect Example*. https://github.com/secretkeylabs/sats-connect-example. [Accessed: 8.05.2024]. 2024.

[39] Ningran Li et al. "Bitcoin Inscriptions: Foundations and Beyond". In: *https://arxiv.org/html/2401.17581v1* (2024).

[40] *Non-fungible token - Wikipedia*. https://en.wikipedia.org/wiki/Non-fungible_token [Accessed: (2024.3.20)]. 2024.

[41] *Non-Fungible Token (NFT): What It Means and How It Works*. https://www.investopedia.com/non-fungible-tokens-nft-5115211 [Accessed: (2024.3.20)]. 2024.

[42] *Non-fungible tokens (NFT)*. https://ethereum.org/en/nft [Accessed: (2024.3.20)]. 2024.

[43] Ordinals Development Team. *ord*. https://github.com/ordinals/ord. [Accessed: 8.05.2024]. 2024.

[44] Financial Times. *What are non-fungible tokens and how do they work?* https://www.ft.com/content/852b7961-51ee-43a3-8caf-f39bb479655c [Accessed: (2024.3.20)]. 2024.

[45] *What are NFTs and why are people paying millions for them?* https://theconversation.com/what-are-nfts-and-why-are-people-paying-millions-for-them-157035 [Accessed: (2024.3.20)]. 2024.

[46] *What are the Functions of Non-Fungible Tokens?* https://www.nftically.com/blog/what-are-the-functions-of-non-fungible-tokens/ [Accessed: (2024.3.20)]. 2024.

[47] *Which blockchains does Rarible support?* https://help.rarible.com/hc/en-us/articles/10457638858253-Which-blockchains-does-Rarible-support. [Accessed: 08.04.2024]. 2024.

[48] *Opensea Automatically Closes Support Tickets About Stolen Art*. https://www.web3isgoinggreat.com/?theme=artTheft&id=opensea-automatically-closes-support-tickets-about-stolen-art. [Accessed: 08.04.2024].