Non-fungible tokens

Description and deployment on ethereum blockchain

UPF Blockchain Technologies 2023

Index

1. Abstract

In this project, we embark on an extensive exploration of non-fungible tokens (NFTs), placing special emphasis on their description and minting process within the Ethereum mainnet blockchain. Our primary objective is to foster a comprehensive understanding of NFTs, elucidate their underlying technology, and highlight their significance in the digital domain. Culminating in the creation of our own unique line of NFTs.

To start talking about what is and how works an NFT will be correct to know about it's history, so first we delve into the story of NFTs, tracing their origin, evolution and their remarkable rise to prominence across various industries. By analyzing their big potential, we will explain the unique characteristics that set NFTs apart from the classical cryptocurrencies exploring the reasons of their popularity and engagement that they had in this modern times.

Digging deeper into the technical aspects we will unravel the way that NFTs work. We examine the underlying blockchain technology that powers them, highlighting the decentralized nature and immutability provided by the Ethereum mainnet. Through the study of different papers, research articles and relevant literature, we will clarify the core components of an NFT, including the smart contracts that govern their behavior, the metadata that defines their properties and the token standards commonly used to ensure compatibility and interoperability.

Furthermore, we navigate the minting process of NFTs on the Ethereum mainnet, analyzing it and then taking it into practice when creating our line of NFTs. We discuss the creation of NFT contracts, the generation of tokens that are unique and the incorporation of metadata to them, all this in the secure and established Ethereum ecosystem. Seen it in a practical example in the implementation part of the project.

In addition to the technical aspects, we delve into the social impact of the NFTs. Taking into account their impact on art, collectibles, examining their role in making creative expression. We also investigate the challenges that arise in ensuring the origin and authenticity of digital assets in the modern age. Taking into the possibility that NFTs can be a new and modern way of art in this digital world.

By exploring all these areas of the NFTs we intend to contribute to the growing body of knowledge surrounding NFTs and their description and minting process on the Ethereum mainnet. Providing readers with a comprehensive resource, culminating with the practical example of how to create a unique line of them. We expect to involve the reader into the digital world of NFTs.

2. Introduction

2.1 Definition

To comprehend the captivating world of non-fungible tokens (NFTs), it is essential to explore not only their definition but also their origin and historical journey. NFTs have disrupted traditional notions of ownership and revolutionized various industries, from art to collectibles and beyond. In this introduction, we will delve into the fundamental aspects of NFTs, their

emergence, and the driving forces behind their remarkable rise, drawing upon noteworthy reference articles and research papers.
NFTs represent unique digital assets that cannot be replicated or have exact copies on a one-to-one basis, setting them apart from fungible cryptocurrencies like Bitcoin, Ethereum or Solana. Each NFT possesses distinct and unique characteristics, properties and ownership rights, enabled thanks to the implementation of blockchain technology. With this technology is ensured the security and transparency of transactions, providing a decentralized ledger for recording and verifying ownership. In essence, NFTs bring together the capabilities of blockchain and digital art, transforming our perception and interaction with digital assets, and creating exciting opportunities for ownership and creative expression.

2.2 Story of NFTs

2.2.1 The first NFT

In the world of creation, it is often the case that there exists a pioneering entity, and within the realm of non-fungible tokens (NFTs), Quantum holds the distinction of being the first. This NFT was created on the Namecoin blockchain in 2014 by Kevin McCoy. The Quantum NFT features a pixelated octagon that dynamically changes colors and moves like an octopus. Notably, the NFT gained attention when it was auctioned through Sotheby's, fetching an astonishing price of $1.47 million. According to Howell (2023), Quantum showed the challenges that early NFTs had to experience, such as lawsuits for ownership disputes. The problem started because McCoy failed to comply with the need for renewal of registrations on Namecoin in 2015, so at that time the focus was in introducing regulations, so that the ownership dispute would be settled.

2.2.2 The Beginning of NFT trading

After that in 2015, Spells of Genesis was created by Everdream Soft and developed over the Bitcoin blockchain. Being the first blockchain trading-card game, according to Creighton (2022), it helped usher in a new era of gaming, one in which players have true ownership of their digital assets. Containing each cart a different artworks that references a distinct moment in the history of blockchain. From here different NFT lines, making that the popularity of NFTs starts growing over time. The next remarkable one was Rare Pepe in 2016. They played a significant role in the evolution of NFTs, serving as pioneers in the use of NFTs for artwork and initiating NFT trading. They gained mainstream attention and showcased the concept of rarity within NFTs. With the introduction of the Rare Pepe Wallet and later utilization on the Ethereum blockchain, Rare Pepes became more accessible and valuable.

Figure 1: Spells of Genesis carts example by Bitcoinist. Retrieved from: https://bitcoinist.com/own-your-deck-in-spells-of-genesis/

2.2.3 The impact of Axie Infinity

The two next NFT lines that came later in 2017 and have been relevant in NFT history are CryptoPunks developed by LarvaLabs and CryptoKitties developed by Dapper Labs. Both continued introducing artwork for blockchain, making NFTs gain more popularity, incrementing the trading part of NFTs and introducing original interactions like breeding the cats with ETH in CryptoKitties to be traded. Following that, in 2018 came one of the most popular NFTs of all times, being one of the first blockchain games. Axie Infinity is an online video game based around NFTs and Ethereum using a “play-to-earn” model, meaning that users can earn money just for playing the game. Axie gained a lot of popularity introducing new people to the NFT community.

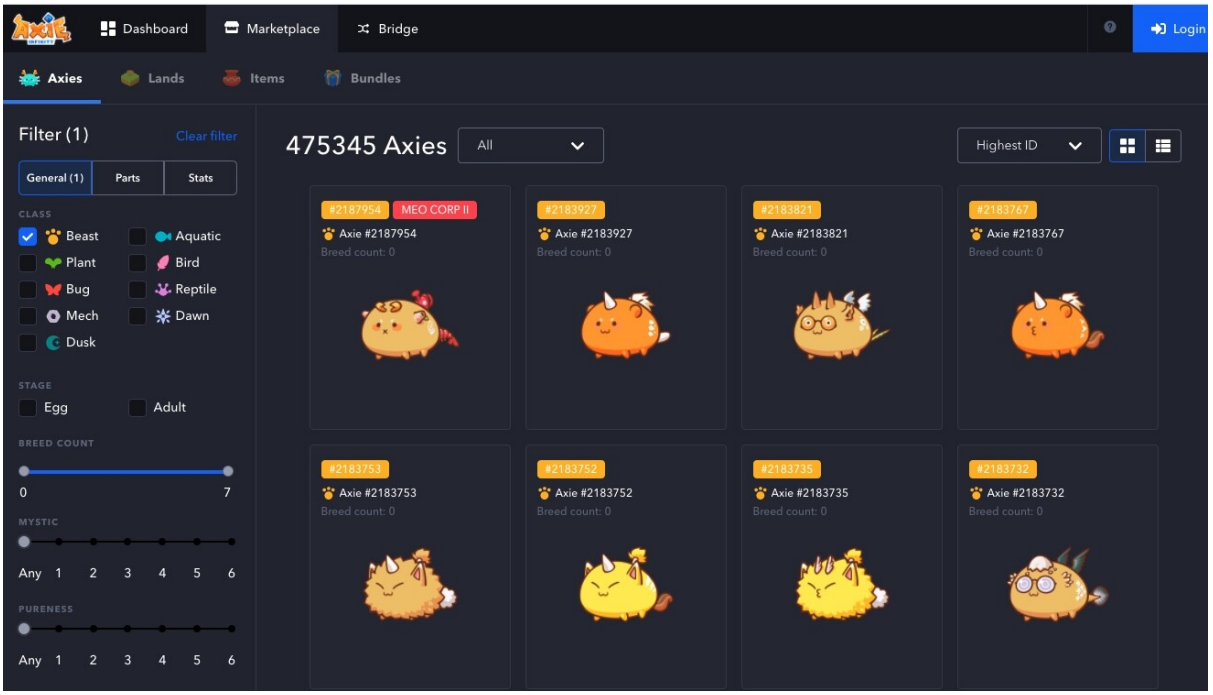


Figure 2: Axie Infinity website example by Enrique Perez. Retrieved from: https://www.xataka.com/videojuegos/axie-infinity-juegos-mayor-crecimiento-ingresos-historia-pokemon-nft-que-vende-que-podemos-ganar-dinero-jugando

2.2.4 The peak of NFTs

From here the NFT community started gaining a lot of popularity, being the most popular and relevant next NFT lines: NBA Top Shot created on 2020, Art blocks created on 2020, and finally one of the most popular NFTs the Bored Ape Yacht Club created on 2021, receiving a massive critical acclaim since its founding thanks to the original art style that they proposed, with most Ape sales going for hundreds of dollars. According to Creighton (2023), being directly responsible for cementing NFTs as a pop culture phenomenon. Transforming NFTs into a popular and common topic of this modern age.

Figure 3: Bored Ape Yacht Club NFT example by Esportmaniacos. Retrieved from: https://www.esportmaniacos.com/otras-noticias/los-monos-nft-bored-ape-yacht-club-desarrollan-un-juego-play-to-earn/

2.3 NFT popularity

After reaching its peak in January 2022, the popularity of NFTs experienced a notable decline, as depicted in worldwide Google search interest for the term "NFT." This temporary drop can be attributed to factors such as market saturation, fluctuating trends, and speculative behavior. However, it is important to consider the broader context and long-term trends, as NFTs continue to show overall growth and expanding adoption across industries. Despite the temporary dip, NFTs remain a transformative force in digital ownership and creative expression, with the potential for enhanced value and provenance as the market matures and regulatory frameworks evolve.

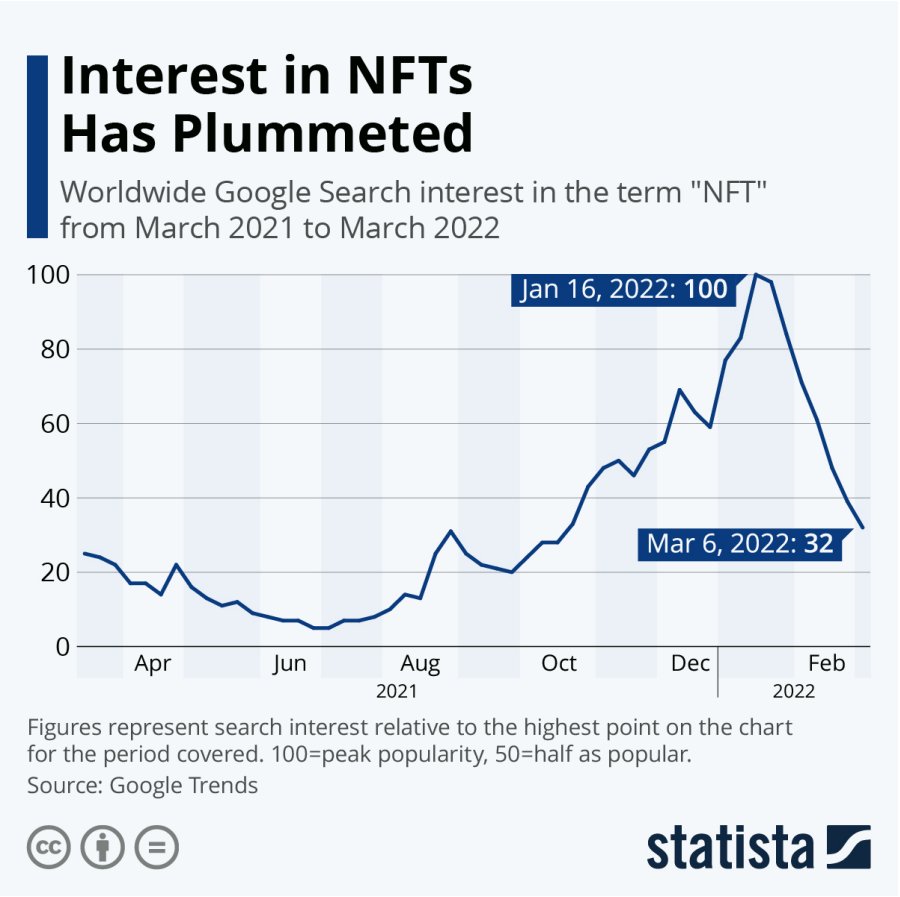


Figure 4: Worldwide Google Search interest in term “NFT” by Statista. Retrieved from: https://www.statista.com/chart/27030/google-search-interest-in-nft/

Following the surge in NFT transactions during the summer of 2021, driven in large part by the success of games like Axie Infinity, the market experienced a notable shift in dynamics. While Axie Infinity emerged as the most valuable NFT collection globally in August 2021 thanks to their innovative style of NFTs in a video game, its sales volume has since seen a decline. However, it is worth noting that the gaming sector has consistently been a dominant force in the NFT market, with significantly higher sales volumes compared to sports-related projects. In fact, in 2020, according to Satista(2022), the gaming segment accounted for approximately 23 percent of the total sales revenue in the NFT market, highlighting the significant role of gaming in driving the adoption and growth of NFTs.

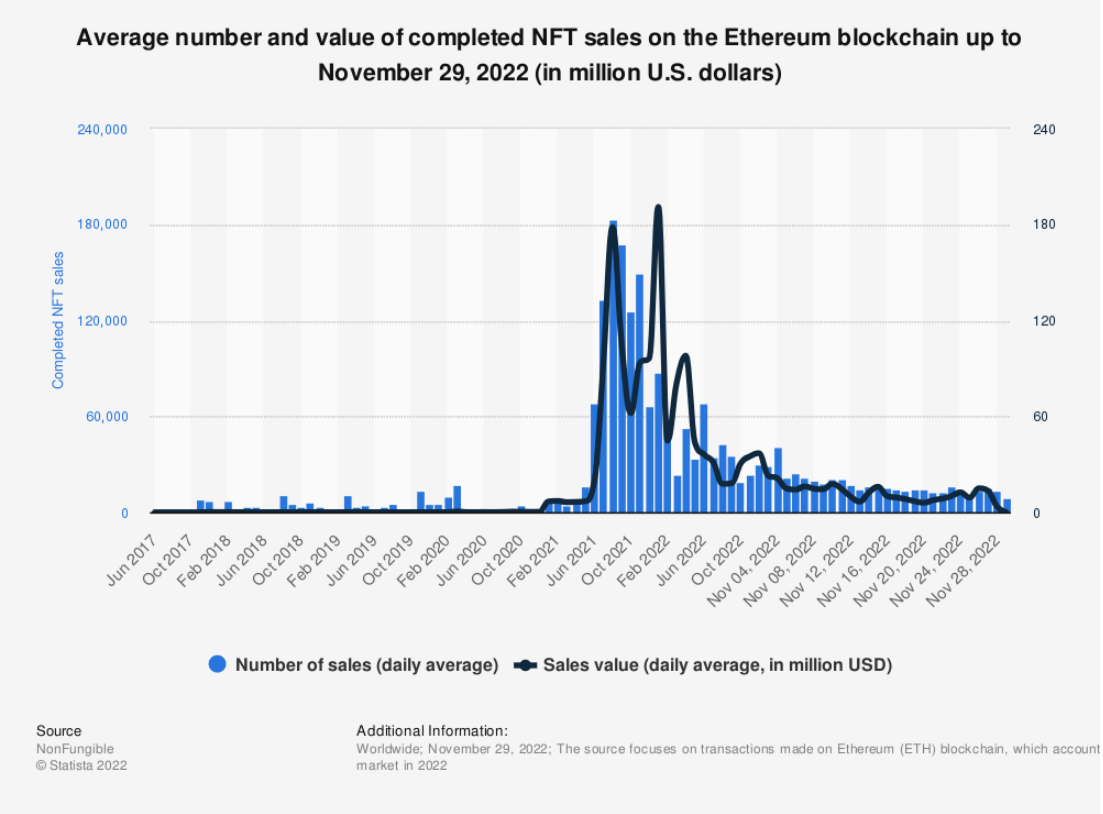


Figure 5: "Average number and value of completed NFT sales on the Ethereum blockchain" by Statista. Retrieved from: https://www.statista.com/statistics/1265353/nft-sales-value/

2.4 The discussion of Art in NFTs

As we saw and mentioned in the story of NFTs, art has always been present, presenting a myriad of possibilities in the digital realm. The potential of NFTs within the art world is vast, according to Casemajor(2022), the NFT format has given rise to the emergence of a new creative scene, providing artists with novel channels for creative expression, ownership rights, and monetization. By creating and selling digital artworks as NFTs, artists gain a digital certificate of authenticity and exclusive ownership privileges. This facilitates direct connections between artists, collectors, and enthusiasts, bypassing traditional intermediaries. Moreover, NFTs introduce the opportunity for artists to receive ongoing compensation through royalties on secondary sales. The exploration of unconventional artistic mediums and the blending of traditional and digital art boundaries are made possible by NFTs. Artists are embracing immersive technologies like virtual reality and augmented reality to craft interactive and experiential artworks that captivate audiences in groundbreaking ways. As artists continue to push creative boundaries and challenge established norms, the potential of NFTs as a pivotal component of the art world continues to expand and evolve.

3. Our Contribution

In the realm of non-fungible tokens (NFTs), our project stands out by offering a unique contribution that encompasses the story of NFTs, their granted popularity, and their big impact on the art world. We go beyond theoretical exploration, explaining the technical

aspects of them, focusing on Ethereum mainnet and provide a practical implementation of a line of NFTs in ERC-721A that exemplifies the transformative potential of NFTs.

Building upon the historical background we have provided, our project actively participates in the art community, utilizing the potential of NFTs to create a distinctive line of digital artwork. By combining our technical prowess with our artistic vision, we have created a collection of NFTs that exemplify the dynamic capabilities and limitless creative possibilities offered by this revolutionary technology.

Through extensive research and doing the implementation, we have gained a lot of insights into the technical aspects of NFTs creation and publication. Our project focuses on exploring and explaining the workings of NFTs, with a particular emphasis on the Ethereum network, where we have done our implementation. We delve into the underlying technology, such as blockchain and smart contracts, that powers the creation, ownership, and transfer of NFTs. By providing clear explanations and practical examples, we shed light on the nuances of Ethereum NFTs and showed the differences between various token standards like ERC-721 and ERC-1155, focusing on ERC-721A.

Familiarizing ourselves with the Ethereum ecosystem, we have understood their complexities, in the different areas such as smart contract deployment, transaction fees, and the decentralized architecture of the Ethereum system. Utilizing our technical expertise, we have successfully created and released a personal line of NFTs made by us on the Ethereum mainnet, showing how it have being done, explaining an step by step process of it, including screenshots and showing too, its far-reaching possibilities for artists, creators, and individuals passionate about the NFT space.

Beyond the creation and publication of NFTs, our project aims to inspire and teach a broader audience, to empower them. We believe that NFTs have the power to disrupt traditional ownership and revolutionize the art industry in any medium that they propose. Through sharing our experiences, insights, and outcomes, we encourage individuals to embrace NFTs as a medium for artistic expression, ownership, and entrepreneurial pursuits.

Through our involvement in the NFT space, we bridge the gap between theory and practice. Our goal is to showcase the possibilities of NFTs, foster connections between artists and collectors, and empower others to embark on their own creative journeys within the growing NFT ecosystem.

Through our comprehensive exploration of the story, popularity, and art of NFTs, and by actively contributing to the NFT space through our own collection, we aspire to make a lasting impact and contribute to the ongoing evolution of this exciting technology.

4. Related work

4.1 Introduction to related work

The related work section provides an overview of the existing literature, research, and projects that are relevant to the technical aspects of our NFT-focused project. In this section,

we explore the advancements and contributions made by previous works in the field of NFTs, specifically emphasizing the technical intricacies and innovations that have shaped the landscape. We delve into various aspects such as smart contract development, token standards, interoperability challenges, scalability solutions, and decentralized storage mechanisms. By examining the related work, we aim to position our project within the broader context of NFT research and development, highlighting its unique contributions and building upon the knowledge established by previous endeavors.

4.2 Smart contract development

To talk about smart contracts we firstly would have to define them. In a few words, a smart contract is a self-executing digital agreement that automatically enforces and facilitates the terms and conditions of a contract between parties on a blockchain network. Several studies have studied smart contracts to know how they work, their challenges and the technical advances of them. Zheng et al. (2019) conducted a comprehensive study about smart contracts, defining the life cycle of smart contracts with their respective phases, and how the development of them works, mentioning their challenges and advances. But not focusing on the NFT world. Seen that the life cycle is composed of 4 phases: creation, deployment, execution and completion. Where in the creation phase parties negotiate the agreement that the software engineers turn into a computer-based smart contract, then in the second phase the contract is deployed in the blockchains platform becoming immutable and accessible to all parties involved, reaching the final phase in the third one the contract is monitored and evaluated executing automatically the contractual procedures when the conditions are met, resulting in transactions executed and validated by miners, reaching the final phase where the states of the involved parties are updated, transactions and updated states on the blockchains are stored and the digital assets between parties are transferred.

For the development of smart contracts, challenges and advances, Ellul and Revolidis (2023) studied emphasizing in the NFTs world and not in general. In the paper we can see that the development of smart contracts in NFTs shares many similarities to smart contracts in any blockchain application, sharing the same phases explained before, but with considerations like the integration of token standards like ERC-721 and ERC-1155, which are commonly used for representing and managing NFTs. And additionally, NFTs often have unique properties and functionalities; such as individual ownership, provenance tracking, or royalty mechanisms, which may require additional smart contract logic. The challenges of smart contracts, according to Majumdar(2022) are the complexity of developing smart contracts that support the unique characteristics of NFTs and the scalability because of their transaction volume and network congestion. But having notable advances addressing this challenges, emerging solutions and frameworks that facilitates the development and deployment of NFT contracts, like ERC-721 and ERC-1155 that improved the token standards providing more robust and flexible options for representing NFTs, introducing too Layer-2 scaling solutions, such as sidechains and state channels, enhancing the scalability and reducing the transaction costs. Having more advances like cross-chain bridges and interoperability protocols enabling seamless NFT transfer.

4.3 Types of tokens and Token standards

In the NFT world there are several different types of tokens, having different purposes. Another important aspect of NFTs is the token standards, in a few words they are sets of rules and protocols that dictate the functionality, behavior, and interoperability of tokens within a specific blockchain ecosystem. Di Angelo and Salzer (2020) studying the NFT world have written a paper explaining the types of tokens and the token standards, studying the most common ones. They explore the distinction between payment tokens, security tokens and utility tokens, highlighting the need to clarify their differences due to varying regulatory requirements. Payment tokens serve a payment function, while security ones represent assets such as equities or debt claims and utility tokens provide access to applications or services. The authors emphasize the need for integrating legal compliance into token standards, wallets, and exchanges, and highlight the importance of a more detailed token classification scheme to address the hybrid characteristics of tokens in the NFT ecosystem.

In the paper it is mentioned that the NFT community engages in discussions and standardization efforts for token interfaces, primarily using the Solidity programming language on the Ethereum blockchain. From these discussions accepted token standards emerge. There are several token standards, ERC-20 the most prevalent and general, followed by ERC-721 that focus on unique tokens that enable the tracking of distinct assets, with individual ownership tracking as a requirement. Then we have ERC-777, which builds upon ERC-20 offering advanced features. And finally ERC-1155, that allows for the management of combinations of fungible and non-fungible tokens within a single contract, supporting simultaneous transfers of multiple token types. Each standard specifies a set of mandatory functions and events that compliant tokens must implement, the only token standard used for NFTs are ERC-721, ERC-1155 and derivations of them created by blockchain users. That is because the other token standards are fungible, and as the name says, NFTs are non-fungible tokens. At last I would like to clarify that we use ERC-721A for the project, being it an updated version of the ERC-721. But the difference between and why we used it will be explained later.

4.4 Interoperability

Interoperability is an important aspect of NFTs, being the ability of different systems, networks, or platforms to seamlessly exchange and utilize information or assets, allowing for seamless communication and interaction between disparate entities. Bishnoi and Bhatia (2020) investigated it, doing a paper presented in the International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE) in 2020. In there they explain blockchain interoperability and solutions for it, but not focusing on NFTs. Even that in the paper the authors discuss how interoperability enables seamless interaction and utilization of services across different platforms, encompassing activities like data referencing, verification, and computational capacity usage, with benefits including asset exchange, cross-chain asset transfer, and the utilization of cross-chain oracles.

Like in the previous paper, Mohanty et al. (2022) offered solutions to improve the interoperability. Explaining that Interoperability solutions in the context of blockchain involve various approaches to enable seamless communication and interaction between different blockchain platforms. Notary scheme solutions focus on utilizing a trusted third party or a decentralized mechanism to verify and authenticate transactions across multiple chains. Sidechain/relay solutions involve the creation of separate chains or relays that facilitate the

transfer of assets and information between different blockchains. Smart contract solutions leverage programmable contracts to establish rules and protocols for cross-chain interactions. Bridging solutions aim to bridge the gap between different blockchain networks by establishing connections and enabling the transfer of assets. Finally, blockchain router solutions provide routing mechanisms that allow for the exchange of data and transactions between disparate blockchains. These solutions address the challenges of blockchain interoperability and promote seamless integration and communication among different blockchain platforms.

4.5 Scalability solutions

Another important aspect of blockchain and obviously that means NFT world is Scalability, that is in a few words the ability of a system or technology to handle increased demands, workloads, or growth efficiently, without compromising its performance or functionality. Chauhan et al. (2018) investigated scalability, contributing to the explanation of it. In it explains that over time, blockchain is becoming more mainstream and with that comes that the number of transactions increase, where in the figure below we can see that cryptocurrencies are being adopted at a very fast rate, coming with it more issues, being the major issue of scalability.

Figure 6: A graph denoting the increase in ethereum transactions from 2016-2023 by Etherscan.io. Retrieved from: https://www.binance.com/en/feed/post/145147

Eventually, it is the miners who become the bottleneck in the transaction process, then because the number of transactions increased the waiting time for the transaction increased a lot. To solve this issue, the developers of Bitcoin are proposing a new Lightning protocol to speed up the process of verification.

Delving deeper in the solutions of this problem nowadays, Zhou et al. (2020) studied strategies to solve this issue, They mention that proof-of-work (PoW) poses challenges for scalability due to its resource-intensive nature, limiting transaction throughput and increasing network congestion, because of that proof-of-stake (PoS) was introduced, offering advantages by reducing the need for resource-intensive mining, allowing for higher transaction throughput and improved network efficiency. Finalizing with Delegated proof of stake (DPoS) that enhances scalability by utilizing a smaller set of trusted nodes, known as

delegates, to validate transactions, thereby increasing transaction processing speed and overall network scalability. Similar to them there were various consensus proposed like PBFT, Hybrid consensus, PoA and PoP, being modifications to improve the scalability.

4.6 Decentralized Storage Mechanisms

In recent years, decentralized storage mechanisms have gained significant attention for their potential in revolutionizing data storage in various domains, including the storage of Non-Fungible Token (NFT) data. Khalid et al. (2023) explained and studied the topic, researching it but not focusing only on the NFT world. It explains that decentralized storage mechanics involve the utilization of distributed networks to store and manage the data in a decentralized manner. The data is stored in multiple nodes around the network, where each of them holds a portion of the data, employing cryptographic techniques to ensure the security and integrity of it. It uses consensus algorithms and peer-to-peer communication protocols to access the necessary fragments of the network. This offers advantages such as fault tolerance, data availability, and resistance to censorship. Allowing too for efficient scaling of storage capacity as more nodes can join the network and contribute their resources.

4.7 Related work conclusion

In conclusion, the field of blockchain technology and its application in various domains, including NFTs, has seen extensive research and development. Numerous studies have contributed to the blockchain evolution in different aspects as we have explained before, contributing to a deeper understanding of the technical intricacies and potential challenges of blockchain implementation, making great advances in this popular technology. It is important to note that advancements in blockchain technology directly impacts on the functionality and performance of NFTs, as they are similar on the principles and technical foundations. Therefore it is crucial to stay up-to-date with blockchain research to understand the evolution of NFTs.

5. Background, terminology and Definitions

5.1 Background, terminology and Definitions introduction

To understand the concepts that we will apply in the following sections is important to give background, explain different terminologies and define different aspects related to NFTs. This section will serve readers to understand the fundamental elements that underpin our subsequent discussions. We will delve into more technical aspects and challenges associated with NFTs in the context of blockchain technology. Beginning with the foundational concepts of it, understanding the background of NFTs, following with different terminologies related to the NFT world, and finishing with the definition of important decentralized storage systems.

5.2 Background

5.2.1 Introduction to blockchain technology

Blockchain technology has revolutionized the way digital transactions work by introducing a decentralized and immutable ledger system. As explained by Buterin (2013) in the Ethereum

whitepaper and by Klaus (2017), blockchain operates on the principles of decentralization, immutability, and distributed ledger technology. With decentralization the need for a central authority to validate transactions is eliminated, enabling trust and transparency. With immutability it is ensured that when a transaction is recorded on the blockchain, it cannot be altered. And distributed ledger technology ensures that copies of the blockchain are stored across multiple nodes, making it secure and resilient. Some of the main blockchain spaces are: Bitcoin (BTC) the first one, Ethereum (ETH) the one where we will work and the first introducing smart contracts, Binance Smart Chain (BSC) that tries to provide fast and low-cost transactions, Cardano (ADA) that focuses on security, scalability and sustainability, Polkadot (DOT) that enables interoperability between different blockchains and Solana (SOL) that was designed for decentralized applications and cryptocurrencies being suitable for applications that require high throughput.

Consensus mechanisms play a crucial role in maintaining the integrity and security of blockchain networks. According to Buterin (2017), with those mechanisms the nodes are enabled to reach an agreement on the validity of transactions and the order in which they are added to the blockchain. With consensus the fact that all participants in the network have a shared understanding of the blockchain state is ensured. The two main important consensus algorithms are Proof of Work (PoW) and Proof of Stake (PoS). Being used to achieve consensus in blockchain networks. The first one involves miners solving complex hash functions to validate transactions, while the second one relies on the stake held by participants to determine their voting power in the consensus process, complementing each other on how to achieve consensus.

Understanding these concepts is totally essential to comprehend the potential of blockchain in facilitating secure, transparent, and efficient transactions. Then, they are particularly relevant in the context of NFTs, as they ensure the authenticity, ownership and traceability of unique digital assets.

5.2.2 Evolution of Blockchain

The evolution of blockchain technology began with the introduction of Bitcoin in 2008. It was created by an anonymous individual or group known as Satoshi Nakamoto, being the pioneering application of blockchain. Over the years, blockchain expanded its capabilities beyond digital currencies and ventured into new territories. One of the most significant events was the introduction of smart contracts by Ethereum, being launched in 2015, they popularized smart contracts, enabling developers to build decentralized applications (DApps) on its blockchain. Smart contracts are basically self-executing agreements with predefined rules and conditions encoded on the blockchain.

Despite the revolutionary potential, according to Dabbagh et al. (2019), early blockchain systems faced a lot of challenges and limitations. Scalability and transaction throughput were the key issues. Seeing that as blockchain networks started growing in popularity , the limited capacity to process a large number of transactions per second started to become evident. To put an example we can talk about Bitcoin. They faced scalability challenges with its proof-of-work consensus mechanism, resulting in a lot slower confirmations and higher fees during the peak usage periods of the blockchain. One of the other challenges that blockchain faces was to achieve a balance between decentralization and efficiency, that is

because high levels of decentralization often came at the cost of scalability and transaction speed. The focus of the blockchain researchers and developers has been to address these challenges, proposing various scaling solutions and strategies to improve scaling and increase the transaction throughput.

5.2.3 Blockchain Applications

Blockchain over the years has been continuously founding applications in different industries, showcasing its potential for innovation and disruption. As said in Jaoude and Saadé (2019), in the finance sector, it has been leveraged to create decentralized digital currencies like Bitcoin, enabling secure and efficient peer-to-peer transactions without intermediaries. In addition, it has facilitated decentralized finance (DeFi) platforms, offering different kinds of services like lending, decentralized exchanges and yield farming. These applications provide users a greater control over their financial assets while reducing the traditional financial institutions.

Beyond the finance aspect, one of the notable areas where blockchain impacted is supply chain management. That is because blockchain enables end-to-end traceability and transparency. It records every transaction and movement of goods on the immutable blockchain, making sure that stakeholders can verify the authenticity of and provenance of the products, ensuring ethical sourcing and reducing counterfeiting. Another industry that not everybody knew that blockchain impacted is healthcare. Through blockchain-based electronic health records, the patient data can be securely stored and shared, enabling interoperability between different healthcare providers while maintaining patient privacy and data integrity.

Furthermore, the rise of Non-Fungible Tokens (NFTs) has captured attention across various industries, including art, gaming, and entertainment. According to Rehman et al.(2021) NFTs utilize blockchain technology to certify the uniqueness and ownership of digital assets, ranging from artwork and collectibles to virtual real estate and in-game items. Opening new avenues for artists, creators and gamers to monetize their digital creations, establish verifiable ownership, and engage with a global audience. As we have seen, the application of blockchain technology in these industries shows totally the versatility and potential that blockchain has beyond the finance aspects.

5.3 Terminology and Definitions

5.3.1 Blockchain Terminology and Definitions

To understand blockchain technology, it is important to familiarize oneself with key terms and concepts that are integral to its operation.

· **NFTs:** Non-Fungible-Tokens are unique digital assets that represent ownership or proof of authenticity of a specific item or piece of content on a blockchain.

· **Tokenization:** It refers to the process of converting real-world or digital assets into NFTs, enabling them to be securely stored and transferred on a blockchain.

· **Consensus mechanisms:**Those mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS), determine how new blocks are validated and added to the blockchain.

· **Cryptographic hashing:** It involves the transformation of data into fixed-length has values using cryptography algorithms, ensuring data integrity and enabling blockchain verification.

· **Public and Private keys:** They are cryptographic tools that secure communication and ownership, being then important in the NFT world. Where public keys act as addresses for receiving funds or messages, while private ones grant access to control and transfer digital assets.
· **Transactions:** They are the core units of data in blockchain, representing the transfer of assets or information between participants of the blockchain.
· **Mining:** The process in which miners solve hash functions, it is essential for adding new blocks to the blockchain.
· **Nodes:** They are the participants or computers in the network, validating transactions, propagating information and contributing to the decentralization and security of the blockchain ecosystem.
· **Smart Contracts:** They are the self-executing contracts with predefined rules and conditions encoded on the blockchain. In this way the terms of agreement are facilitated, verified and enforced without the need for intermediaries.
· **Decentralization:** The distribution of authority and control across the network of participants rather than relying on a central authority. This is the core principle of blockchain.
· **Immutable:** Refers to the unchangeable and tamper-resistant nature of data recorded on the blockchain. That means that once information is added to the blockchain, it cannot be altered or deleted.
· **Fork:** Is a split in the blockchain network, resulting in the creation of two or more separate chains with different rules and histories. They can be hard forks that create a permanent divergence, or soft forks, which are temporarily backward-compatible.
· **Wallet:** It is a digital application or device used to store, manage and interact with blockchain-based assets. These wallets store in a secure way the private keys and allow users to send and receive cryptocurrencies and other digital assets.
· **Token Standards:** They refer to the predefined rules and specifications that govern creation, behavior and interoperability of tokens on a blockchain network, ensuring compatibility and standardization among tokenized assets.
· **Mint:** It is the process of creating and issuing a unique digital asset on a blockchain, establishing its authenticity and ownership.
· **Ownership:** It refers to the legal or rightful possession and control over a property, asset, or item, entailing the rights and responsibilities associated with its use, transfer, and disposition.
· **Royalties:** They are a percentage of subsequent sales or transactions that are automatically paid to the original creator or rights holder of an NFT whenever it is resold.
· **AirDrop:** Functionality that allows the owner of a token collection to mint instances directly to a chosen wallet without cost (gas fees still apply).
· **Metadata:** The information about a determined token stored in a .json file, hosted on a decentralized network. For different collections they may contain different attributes, but some standards are the name, id, description and (link to) assets related to the NFT.
· **Test Network:** Testnets are test blockchain networks that act and perform similarly to the main networks (mainnets) they are associated with. Since they operate on separate ledgers from the mainnet, the coins on a testnet have no connection to transactions and value on the mainnet.

5.3.2 Decentralized Storage Terminology and Definitions

To understand decentralized storage underlying concepts, several keys and terms are essential for doing it.

· **Data Redundancy:** Refers to the practice of storing multiple copies of data across different nodes or devices, ensuring that data remains available even if some nodes fail.
· **Content Addressing:** It is a method of uniquely identifying data based on its content, typically through the use of cryptography hashes.
· **Distributed File Systems:** They enable the storage and retrieval of files across multiple nodes in a decentralized network, facilitating fault tolerance and scalability.
· **Peer to Peer:** They are basically decentralized networks where participants, known as peers, interact with each other without intermediary.

Examples of decentralized storage solutions:
· **IPFS:** InterPlanetary File System is a protocol that enables the creation and retrieval of content-addressed, distributed file systems. Using a peer-to-peer network to store and share data. In this way it provides a resilient and censorship-resistant storage solution.
· **Swarm:** Is a decentralized storage and content distribution platform built on top of the Ethereum blockchain, aiming to provide incentivized storage and content retrieval, allowing users to host and access data in a secure and efficient manner.
· **Filecoin:** It utilizes blockchain technology to create a marketplace for storage providers and users. Incentivizing participants to contribute their storage space and bandwidth, forming a robust and decentralized storage ecosystem.

6. Crypto Croakers - introduction

Crypto Croakers (CRK) is the name of the NFT collection that has been developed and deployed for this project as a practical application, it is an ERC-721A type non-fungible token on the ethereum Goerli blockchain with 50 mintable instances (while there are enough assets for 4000+ tokens many of the programs used impose paywalls for larger number of files, therefore we have settled for a smaller collection size). CryptoCroakers, like many other simpler NFT projects, have no real purpose other than to collect them or use them as a profile picture in social media services, they are not associated to any kind of web3 service or game (other than NFT marketplaces).
ERC-721A has been chosen as it is an improvement over the dedicated non-fungible token implementation ERC721 offers, allowing users to mint multiple NFTs in a single transaction for essentially the same cost of minting a single one which is much more costly for ERC721 tokens. A modified version of the NFT contract template developed by Marco Lipparini has been used under MIT license, it takes care of some functionality like the deployment and verification of the smart contract through generic scripts.

We will explain the process of designing, creating and deploying the project on a test network along with relevant information in relation to the previous sections of this paper and determine the price to pay were we to apply the process on the main ethereum network at the time of writing.

The programs and services used throughout the development of Crypto Croakers are the following:
pinata.cloud: IPFS access, data storage
nft-inator.com: NFT metadata generation
Infura.io: managing project connections and endpoints

Etherscan.io: block explorer; consult contract address, transaction hashes and interact with contract
goerli-faucet.pk910.de: obtain funds for Goerli test network
Opensea.io (testnets): collection configuration and NFT marketplace

All wallets, keys and assets have been created with the sole objective of realizing this project. Some of the data shown in the implementation description might be compromising information that could lead to losing access to a project and should not be disclosed under any circumstance were it to be a commercial project.

7. Implementation Description

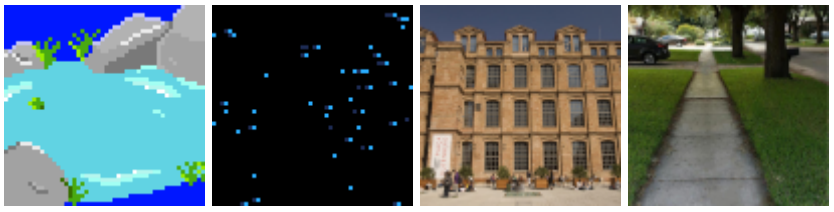
7.1 Creating the art

7.1.1 Design specifics

Each token is displayed in a small 100x100p canvas with a simple pixel art aesthetic, it was decided to be this simple to facilitate creating original assets without spending a large amount of time, the low image size also makes it easier to upload them to the IPFS protocol. We decided to base the design around frogs because they are iconic, simple to draw and there are many types of them in nature to pull inspiration from.

7.1.2 Creative process

For this project we have used a layered approach to the art creation process, as it allows us to create a large variety of pictures with visual cohesion and easily recognizable silhouettes with few assets. Many of the more popular projects such as cryptopunks or the bored ape yacht club use this same method, as it's much more time efficient than creating each possible token one by one.
These are the attributes that compound a Crypto Croaker, along with the total amount of items that have been designed for each one:

Background - 4 items

Base - 5 items


Face - 4 items

Eyes - 4 items

Accessory - 4 items (including empty)

Hat - 4 items (including empty)

Final appearance examples


Aside from the tokens themselves, a generic image and a background showcasing some of the available CryptoCroakers has been made.

Figure 7: Collection icon and banners, will be shown when browsing the collection through OpenSea.

7.2 From picture to NFT

There are two key elements needed to publish the collection:

1. The desired amount of pictures obtained by combining different layers
2. The corresponding metadata for each picture

The metadata for each individual image is stored on a json file and contains relevant information about their corresponding token (name, symbol, brief description, corresponding image and attributes,...) along with an extra json containing information about the entire collection.

The process of creating each individual file is quite long and time-consuming for large collections, so we used the free platform NFT-inator to handle the creation of finalized images and relevant metadata. There are many web or script alternatives for this process.
For our collection the metadata contains information about each of the layers that make up the image, a link to the image hosting in IPFS (more details below), and a small description for the token and the token name (containing its corresponding ID)

```
{
  "name": "Crypto Croakers #1",
  "image": "ipfs://QmRtVG3xdUgNc5NhWZJ1e75wsTGdRqfcPgo15tNUvpr1t8/1.png",
  "description": "Crypto Croakers have come from their local pond all the way to your wallet. This frog has croaked 1 time.",
  "external_url": null,
  "attributes": [
    {
      "trait_type": "Hat",
      "value": "Hat000"
    },
    {
      "trait_type": "Accessory",
      "value": "Accessory001"
    },
    {
      "trait_type": "Eyes",
      "value": "Eyes000"
    },
    {
      "trait_type": "Face",
      "value": "Face003"
    },
    {
      "trait_type": "Base",
      "value": "Base001"
    },
    {
      "trait_type": "Bg",
      "value": "Bg001"
    }
  ],
  "seller_fee_basis_points": 0,
  "compiler": "nft-inator.com"
}
```


Figure 8: Metadata for the token with id 1


```
{
  "name": "Crypto Croakers #26",
  "image": "ipfs://QmRtVG3xdUgNc5NhWZJ1e75wsTGdRqfcPgo15tNUvpr1t8/26.png",
  "description": "Crypto Croakers have come from their local pond all the way to your wallet. This frog has croaked 26 times.",
  "external_url": null,
  "attributes": [
    {
      "trait_type": "Hat",
      "value": "Hat002"
    },
    {
      "trait_type": "Accessory",
      "value": "Accessory002"
    },
    {
      "trait_type": "Eyes",
      "value": "Eyes003"
    },
    {
      "trait_type": "Face",
      "value": "Face003"
    },
    {
      "trait_type": "Base",
      "value": "Base000"
    },
    {
      "trait_type": "Bg",
      "value": "Bg002"
    }
  ],
  "seller_fee_basis_points": 0,
  "compiler": "nft-inator.com"
}
```


Figure 9: Metadata for the token with id 26

In addition to each individual token and the collection, we also create an image and metadata for a hidden token which will be displayed to all CRK holders that acquire their

NFT before the collection is revealed. Collections normally use this feature to avoid speculation with the tokens before they're made available to all consumers, as it obscures the attributes of the token making it impossible to determine it's rarity; for this project, all attributes have the same appearance frequency and there will be no real buyers apart from the token creators during the presale period so the feature has no real use, however for the sake of the project's completeness and documentation it was implemented.


```
{
  "name": "Crypto Croakers #??",
  "image": "ipfs://Qmd8hoZF8tqVFJZmvrPNiD4h3ow3ySGG2ojSnmrZRHFXbB/hidden01.png",
  "description": "Wonder what this Croaker will be like?"
}
```

Figure 10: Hidden token picture and metadata

Once we have all necessary assets we must upload them to the IPFS protocol, so future CRK holders have access to the picture corresponding to their token. IPFS offers a decentralized peer-to-peer solution to file sharing, meaning we don't have to depend on an external server to host these files so the NFT can't be rendered unusable (having the token but not being able to see the picture associated with it).

7.3 Smart contract development

The first steps to configuring our contract is setting up the basic information: our token's name, symbol and total supply along with the price. The ERC721A structure was used as a standard for creating the token, as it is the case with many other NFT projects.
The contract has functionality for changing token price, activating a whitelist, hidden token compatibility and basic checks before calling the token's mint function, along with relevant methods to allow the contract owners to change certain parameters without having to deploy a whole new contract.

These are the following methods and modifiers of the solution along with a brief explanation;

- **Minting condition checks**

```
modifier mintCompliance(uint256 _mintAmount) {
  require(_mintAmount > 0 && _mintAmount <= maxMintAmountPerTx, 'Invalid mint amount!');
  require(totalSupply() + _mintAmount <= maxSupply, 'Max supply exceeded!');
  _;
}

modifier mintPriceCompliance(uint256 _mintAmount) {
  require(msg.value >= cost * _mintAmount, 'Insufficient funds!');
  _;
}
```

Baseline functionality to prevent tokens from being generated if the minter did not provide sufficient funds or if the collection has already reached the max supply of 50 different CRK tokens.

- **Whitelist mint**

```
function whitelistMint(uint256 _mintAmount, bytes32[] calldata _merkleProof) public payable
mintCompliance(_mintAmount) mintPriceCompliance(_mintAmount) {
  require(whitelistMintEnabled, 'The whitelist sale is not enabled!');
  require(!whitelistClaimed[_msgSender()], 'Address already claimed!');
  bytes32 leaf = keccak256(abi.encodePacked(_msgSender()));
  require(MerkleProof.verify(_merkleProof, merkleRoot, leaf), 'Invalid proof!');

  whitelistClaimed[_msgSender()] = true;
  _safeMint(_msgSender(), _mintAmount);
}
```

Allow for addresses manually added to the whitelist to claim tokens at a different (lower) price (ONLY during the whitelist sale period). Each address may only use this function once to avoid bad actors, calls the token's mint function if the requirements and conditions are met.

- **baseline mint**

```
function mint(uint256 _mintAmount) public payable mintCompliance(_mintAmount) mintPriceCompliance(_mintAmount) {
  require(!paused, 'The contract is paused!');

  _safeMint(_msgSender(), _mintAmount);
}
```

The function regular users have to use in order to become CRK holders. If the contract is running correctly and conditions are met, a new token will be minted to the address calling the function.

- **privileged mint**

```
function mintForAddress(uint256 _mintAmount, address _receiver) public mintCompliance(_mintAmount) onlyOwner {
  _safeMint(_receiver, _mintAmount);
}
```

Alternative minting function for contract owner, allows for airdropping tokens to a desired address.

- **get token metadata**

```
function tokenURI(uint256 _tokenId) public view virtual override returns (string memory) {
  require(_exists(_tokenId), 'ERC721Metadata: URI query for nonexistent token');

  if (revealed == false) {
    return hiddenMetadataUri;
  }

  string memory currentBaseURI = _baseURI();
  return bytes(currentBaseURI).length > 0
      ? string(abi.encodePacked(currentBaseURI, _tokenId.toString(), uriSuffix))
      : '';
}
```

Returns the link to a token's metadata, will check if the collection has been revealed to set the true token's features or the generic hidden token features.

- **contract management functions**

```
function setCost(uint256 _cost) public onlyOwner {
  cost = _cost;
}

function setMaxMintAmountPerTx(uint256 _maxMintAmountPerTx) public onlyOwner {
  maxMintAmountPerTx = _maxMintAmountPerTx;
}

function setHiddenMetadataUri(string memory _hiddenMetadataUri) public onlyOwner {
  hiddenMetadataUri = _hiddenMetadataUri;
}

function setUriPrefix(string memory _uriPrefix) public onlyOwner {
  uriPrefix = _uriPrefix;
}

function setUriSuffix(string memory _uriSuffix) public onlyOwner {
  uriSuffix = _uriSuffix;
}

function setPaused(bool _state) public onlyOwner {
  paused = _state;
}

function setMerkleRoot(bytes32 _merkleRoot) public onlyOwner {
  merkleRoot = _merkleRoot;
}

function setWhitelistMintEnabled(bool _state) public onlyOwner {
  whitelistMintEnabled = _state;
}
```

A slew of functions available to the owner used to change the contract's parameters and permissions once it has been deployed.

The ERC721 token structure has some base functionalities like renouncing/transferring ownership of the contract which will also be available to use by the owner once it's deployed correctly.

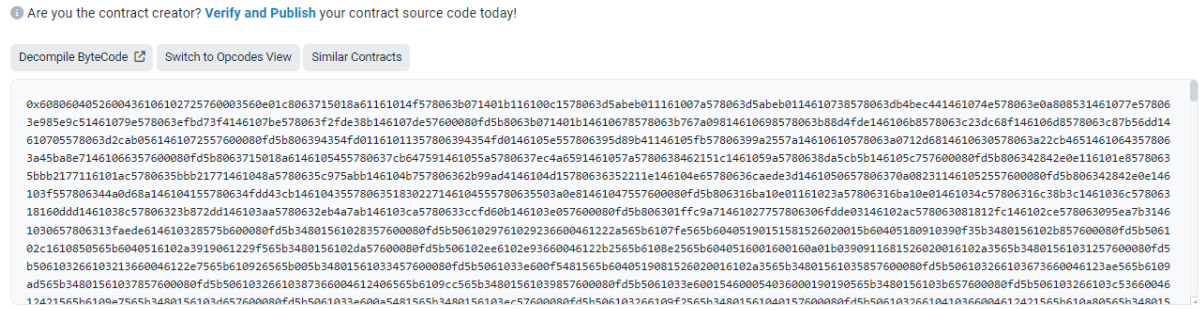
Now that the contract is set up correctly, we must configure the necessary connections and dependencies. We will do this through the .env file that will not be uploaded to the github to avoid revealing compromising information.
First we load the IPFS address of our tokens' metadata so the contract can actually contain the NFTs, remember the image file link for each image is found in its corresponding data file, furthermore to claim ownership of the contract before deploying it's necessary to obtain the desired address' private key and specify it in this file, this can be done directly from metamask.
We must also set up the endpoints for both the main network and a test network (for this project we will be using Goerli), to do this we first generate the API keys for the project using Infura and obtain the links to the desired networks.
There has to be an Etherscan API key associated with the project for the contract to be correctly tracked and validated, so that information will be specified here as well.
An example address was added to the whitelist to test the whitelist feature, but more can be added if necessary after contract deployment.

7.4 Deployment on Goerli network.

The advantage of test networks is that there is no real monetary risk, as the network's respective currency can be obtained relatively easily for free.
For our test, we obtained a sample of GöETH from a PoW faucet publicly available.
Deploying the contract:

```
yarn run v1.22.19
$ hardhat run scripts/1_deploy.ts --network testnet
No need to generate any newer typings.
Deploying contract...
Contract deployed to: 0xC515362B1875304d6E40cF9CbF7475A7522Ea930
Done in 18.86s.
```

Once the contract has been deployed we get an associated contract address, however if we check the address on etherscan we can see the contract has not yet been verified.



We can easily circumvent this by using some features provided by Marco Lipparini's baseline ERC721 contract, which take care of the process.

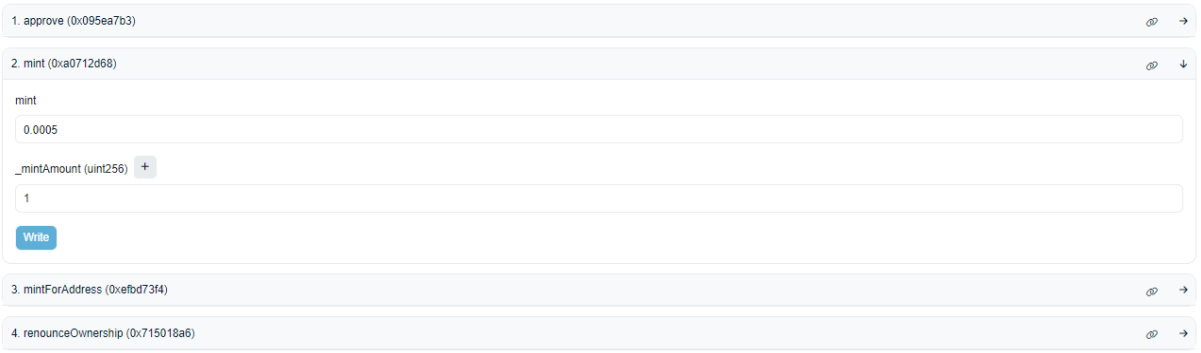
```
yarn run v1.22.19
$ hardhat verify --constructor-args config/ContractArguments.ts 0xC515362B1875304d6E40cF9CbF7475A7522Ea930 --network testnet
Nothing to compile
No need to generate any newer typings.
Successfully submitted source code for contract
contracts/CryptoCroakers.sol:CryptoCroakers at 0xC515362B1875304d6E40cF9CbF7475A7522Ea930
for verification on the block explorer. Waiting for verification result...

Successfully verified contract CryptoCroakers on Etherscan.
https://goerli.etherscan.io/address/0xC515362B1875304d6E40cF9CbF7475A7522Ea930#code
Done in 13.08s.
```

Now that the contract has been verified it can be viewed publicly and interacted with on a block explorer compatible with Goerli (e.g. etherscan), it can be accessed from here.

To allow NFT minting functionality, a sale period has to be started first (as the contract is paused on initialization). As the owner, we can update the contract to have a sale opened; for this first mint we will open it under a whitelist so only authorized addresses can access it.

There are many ways to mint an NFT now that the contract has been deployed and verified; a simple way would be to call the mint function directly from etherscan.



The transaction was completed successfully! A new event can be seen on etherscan under the CryptoCroakers smart contract with information regarding the block that processed the minting transaction.

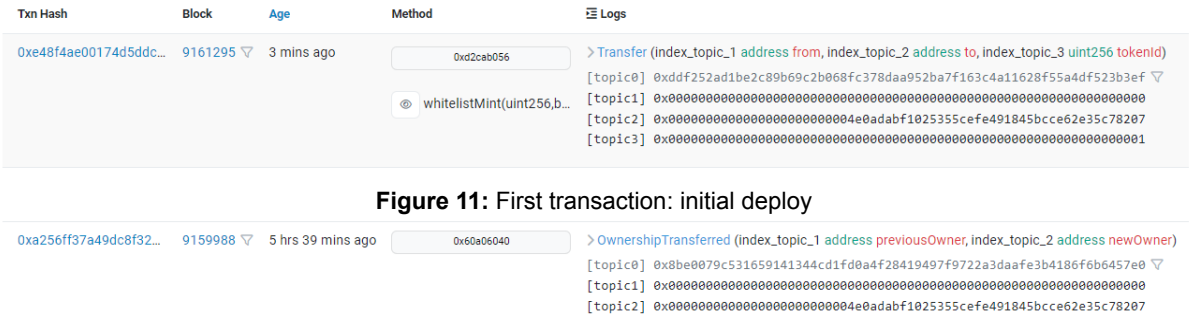


Figure 11: First transaction: initial deploy

Figure 12: Second transaction: first minted token (whitelist period)

With this, the process is almost complete. If we check the newly acquired Crypto Croaker on OpenSea testnets, it can be observed that the token's image, id and description show generic 'hidden token' information.

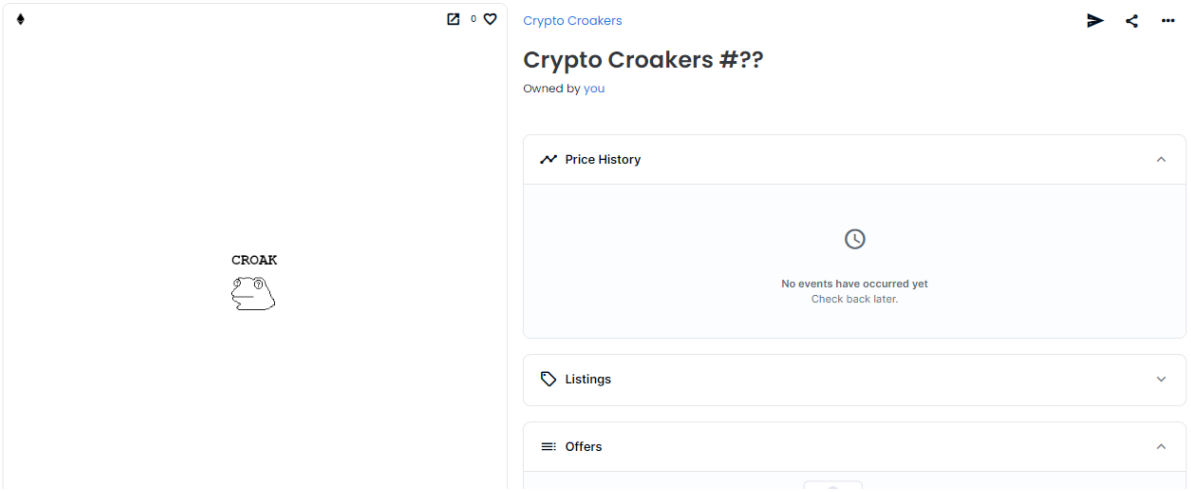


Figure 13: first minted token as seen on OpenSea

The collection has not yet been revealed, therefore all minted NFTs will not display their true data. This status is determined by a boolean in the smart contract, which as the owners we can easily change using the corresponding method from etherscan.

The project is now complete, and all acquired tokens can be viewed on web3 marketplace apps that are compatible with the Goerli test network. A few tokens were minted and put on sale as a test.
[CryptoCroakers testnet collection can be viewed here](#) - you can buy, sell and mint your own!

Figure 14: collection preview

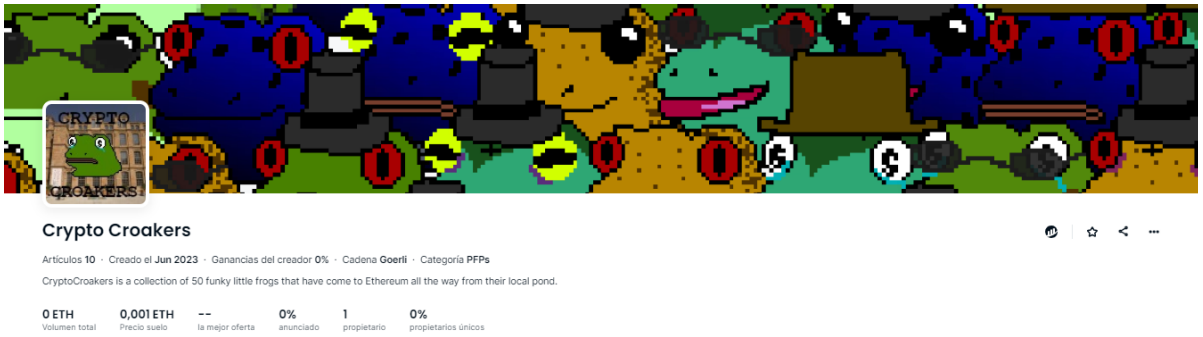
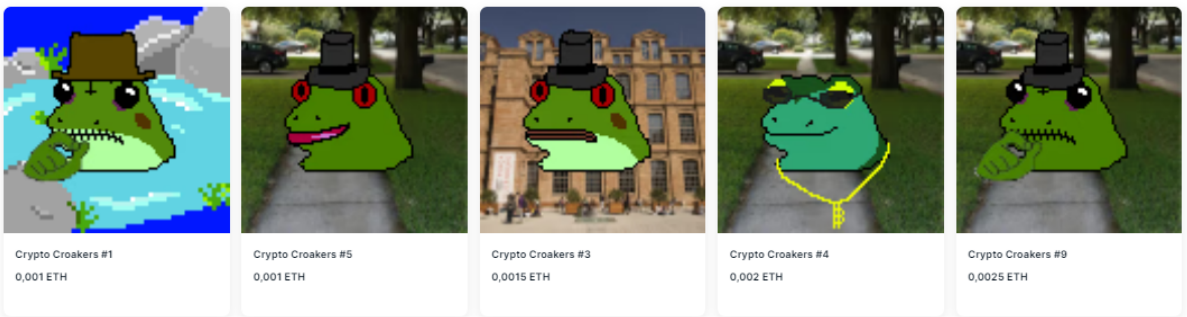


Figure 15: collection banner



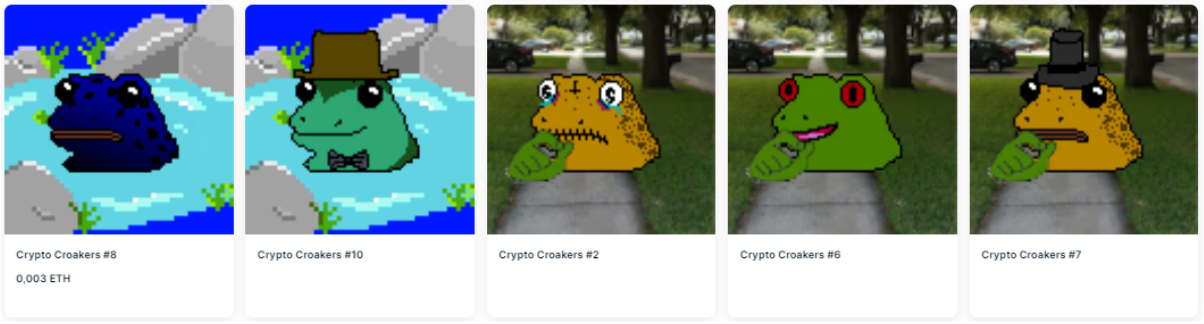
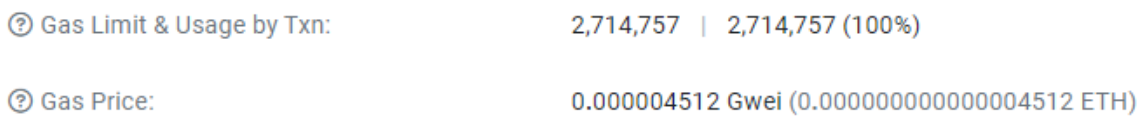


Figure 16: some of the tokens up for sale at the time of writing

https://goerli.etherscan.io/address/0xC515362B1875304d6E40cF9CbF7475A7522Ea930#code
https://testnets.opensea.io/collection/crypto-croakers

7.5 Deploying on mainnet

The process of deploying the collection on the main ethereum network is extremely similar to that of the test network, the only difference would be changing the endpoint obtained from Infura from Goerli to the mainnet.
We can get an estimated cost of contract deployment using data gathered from the previous process; first off we check the amount of gas consumed on etherscan.



As can be seen, a total amount of 2.714.757 gas was used, however the displayed gas prices are only accurate for the Goerli network and can't be applied to ethereum. There are many services that track the live values of gas prices for each network, at the time of writing this paper the average gas price over the last 24 hour period is 17.

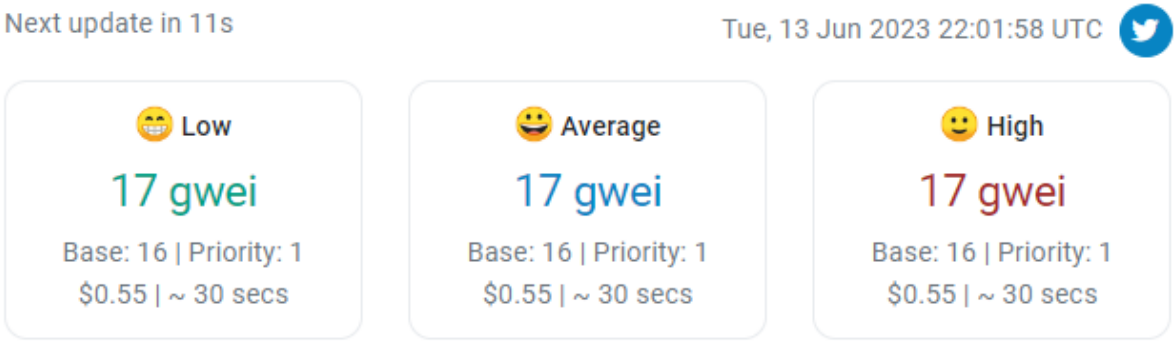


Figure 17: gas tracker service provided by etherscan.io

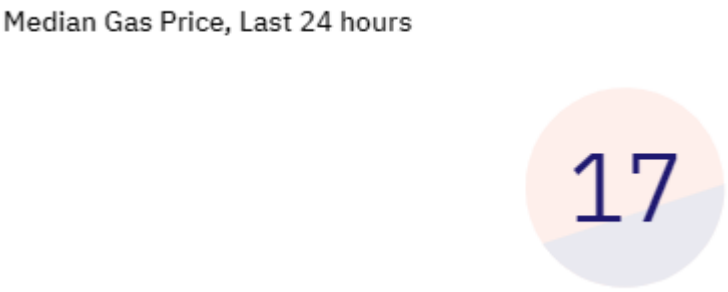


Figure 18: ethereum gas tracker provided by useweb3.xyz

With this information we can mathematically estimate the total price;

2.714.757 * 17 = 46.150.869 Gwei
46.150.869 Gwei = 0.04615 ETH

The final price is about 75€ at the time of writing, without accounting for minting prices and royalties, which is outside the scope of the project therefore the collection has been uploaded to only the test network as a proof of concept.

References and credit:

· Howell, J. (2023, March 17). A brief history of NFTs. Retrieved from: https://101blockchains.com/history-of-nfts/

· Creighton, J. (2022, December 15). NFT Timeline: The Beginnings and History of NFTs. Retrieved from: https://nftnow.com/guides/nft-timeline-the-beginnings-and-history-of-nfts/

· Casemajor, N. (2022, December 11). NFTs in the art world: A revolution or ripoff? Retrieved from: https://theconversation.com/nfts-in-the-art-world-a-revolution-or-ripoff-191299

· Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X., Weng, J., & Imran, M. (2019, December 22). An Overview on Smart Contracts: Challenges, Advances and Platforms. Retrieved from arXiv preprint arXiv:1912.10370.

·Ellul, J., & Revolidis, I. (2023, January 16). Non-Fungible Tokens (NFTs), Smart Contracts and Contracts: The need for Legal and Technology Assurances. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4325415

·Majumdar, S. (2022, February 25). The challenges of cryptocurrency, NFTs, and smart contracts on litigation. Retrieved from https://www.lexology.com/library/detail.aspx?g=a1a2632d-bb36-4c82-89da-2a9f942e7a14

· Di Angelo, M., & Salzer, G. (2020, July 8). Tokens, Types, and Standards: Identification and Utilization in Ethereum. In 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 1-6). IEEE. doi: 10.1109/ICBC48256.2020.9169177 Revenue from https://ieeexplore.ieee.org/abstract/document/9126009

· Bishnoi, M., & Bhatia, R. (2020, December 8). Interoperability Solutions for Blockchain. Retrieved from https://ieeexplore.ieee.org/document/9277054

· Mohanty, D., Anand, D., Aljahdali, H. M., & Villar, S. G. (2022, January 14). Blockchain Interoperability: Towards a Sustainable Payment System. Retrieved from https://www.mdpi.com/2071-1050/14/2/913

· Chauhan, A., Malviya, O. P., Verma, M., & Mor, T. S. (2018, August 13). Blockchain and Scalability. Retrieved from https://ieeexplore.ieee.org/abstract/document/8431962?casa_token=vnDwsIC-dDMAAAAA:oU6Pj2RahlZ-mk2g1WSmeNODgfg404N5674wadd8MDSJgSJx8J4RF3eRCl0EjJNFqwALj-s9

·Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020). Solutions to Scalability of Blockchain: A Survey. IEEE. Retrieved from https://ieeexplore.ieee.org/abstract/document/8962150

· Khalid, M. I., Ehsan, I., Al-Ani, A. K., Iqbal, J., Hussain, S., Ullah, S. S., & Nayab. (2023, January 27). A Comprehensive Survey on Blockchain-Based Decentralized Storage Networks. Retrieved from https://ieeexplore.ieee.org/abstract/document/10026822

· Buterin, V. (2013). Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform. Retrieved from https://ethereum.org/whitepaper/

· Klaus, I. (2017, March 17). Don Tapscott and Alex Tapscott: Blockchain Revolution. *New Global Studies*, *11*(1), 47-53. Retrieved from https://doi.org/10.1515/ngs-2017-0002

· Buterin, V. (2017, October 25). *Casper the Friendly Finality Gadget*. arXiv.org. Retrieved from https://arxiv.org/abs/1710.09437

· Dabbagh, M., Sookhak, M., & Sohrabi Safa, N. (2019, January 29). The Evolution of Blockchain: A Bibliometric Study. IEEE Access, 7, 26291-26301. https://doi.org/10.1109/ACCESS.2019.2896351

· Jaoude, J. B., & Saadé, R. G. (2019). Blockchain Applications – Usage in Different Domains. *IEEE Access*, *7*, 45360-45381. Revenue from https://doi.org/10.1109/access.2019.2902501

· Rehman, W., Zainab, H. E., Imran, J., & Bawany, N. Z. (2021, December 21). NFTs: Applications and Challenges. In *2021 22nd International Arab Conference on Information Technology (ACIT)*. https://doi.org/10.1109/acit53391.2021.9677260

· ERC721a structure documentation and code by Azuki https://www.azuki.com/erc721a / https://www.erc721a.org/