AALBORG UNIVERSITY
COPENHAGEN

Aalborg University Copenhagen
A.C. Meyers Vænge 15
2450 København SV

Semester Coordinator: Henning Olesen
Secretary: Charlotte Høeg

Semester:
4th Semester

Title:
The Case for Authentic Digital Collectibles | A Decentralised Identity Approach for Fine Art

Project Period:
February 2022 - June 2022

Semester Theme:
Master's Thesis

Author:
Dumitrița-Felicia Roșu

Supervisor:
Reza Tadayoni

Pages: 74
Finished: June 02, 2022

Abstract:

Blockchain is one of the areas that witness an increasingly fast pace of development. One of the newest technologies powered by Blockchain is represented by Non-Fungible Tokens or NFTs - unique units of data stored on the DLT, that have lately been trading on various marketplaces for exorbitant amounts.

With a high traction and increased demand, the ecosystem is governed by acute lack of regulation, extensive fraudulent activity and plagiarised content.

Based on a thorough literature review and data collection process, the thesis proposes a secure NFT marketplace that fosters authentic participants and listings, by introducing a mandatory KYC (Know Your Customer) process for users who would like to engage in transactions, their data being encrypted and stored on-chain.

The current paper contributes to existing knowledge by validating the need for a secure context to trade NFTs, by addressing the confusion between an NFT and the media asset that it is linked to, and also by pioneering the approach of on-chain identification in the context of trading Non-Fungible Tokens.

MSc. Thesis

Innovative Communication Technologies and Entrepreneurship

The Case for Authentic Digital Collectibles | A Decentralised Identity Approach for Fine Art

Author
Felicia Roșu
drosu17@student.aau.dk

Supervisor
Reza Tadayoni
reza@es.aau.dk

Thesis Submitted in Partial Fulfilment of the Requirements for the Degree of Master of Science (MSc) in Engineering, Innovative Communication Technologies and Entrepreneurship

June 2022

Abstract

Blockchain is one of the areas that witness an increasingly fast pace of development. One of the newest technologies powered by Blockchain is represented by Non-Fungible Tokens or NFTs - unique units of data stored on the DLT, that have lately been trading on various marketplaces for exorbitant amounts.

With a high traction and increased demand, the ecosystem is governed by acute lack of regulation, extensive fraudulent activity and plagiarised content.

Based on a thorough literature review and data collection process, the thesis proposes a secure NFT marketplace that fosters authentic participants and listings, by introducing a mandatory KYC (Know Your Customer) process for users who would like to engage in transactions, their data being encrypted and stored on-chain.

The current paper contributes to existing knowledge by validating the need for a secure context to trade NFTs, by addressing the confusion between an NFT and the media asset that it is linked to, and also by pioneering the approach of on-chain identification in the context of trading Non-Fungible Tokens.

Acknowledgements

I would like to express my deepest gratitude and appreciation to my supervisor, Reza Tadayoni for his continuous support and precious advice during this academic journey that led me towards an inspiring experience. The completion of this thesis could not reach the destination without his patient guidance and dedication.

Also, I would like to take the chance to thank all the receptive people involved within the data collection and testing phases of the project. Special thanks to both experts in the field for the fruitful discussions.

Last but not least, I would like to express my warmest thanks to Tudor Nastasă for always believing in me, inspiring and motivating me to stay on the path and to accomplish my dreams. And to my parents and my beloved sister, Cristina, for all their support and encouragement throughout my life. Thank you for being there when I needed it the most!

Table of Contents

List of Abbreviations

ABI Application Binary Interface.
AES Advanced Encryption Standard.
AI Artificial Intelligence.
API Application Programming Interface.

dApp Decentralised Application.
DeFi Decentralised Finance.
DLT Distributed Ledger Technology.
DoS Denial of Service.

GUI Graphical User Interface.

IPFS InterPlanetary File System.
IPR Intellectual Property Rights.

JSON JavaScript Object Notation.

KPI Key Performance Indicator.
KYC Know Your Customer.

ML Machine Learning.
MVC Model View Controller.
MVP Minimum Viable Product.

NFT Non-Fungible Token.

OOP Object Oriented Programming.
OSI Open Systems Interconnection.

PEP Politically Exposed Person.
PII Personally Identifiable Information.
PoS Proof of Stake.
PoW Proof of Work.

QA Quality Assurance.

SEC Securities and Exchange Commission.
SSR Server-Side Rendering.

TDD Test Driven Development.
TPS Transactions per second.

UML Unified Modelling Language.

WEF World Economic Forum.

List of Figures

1 Introduction

During the most recent decades, the world witnessed a huge leap in the development of new technologies. Initially, technology was being scaled and applied at an industrial level [1], where aspects such as industrialisation and mass production were fostered by advancement in manufacturing and production technology.

At a later stage, increased digitalisation started to get traction and the modern technology field started to emerge, with software and hardware companies being at the forefront of this massive shift [2]. All this has been enhanced further by the Internet wide spread adoption, that in the first stage was enabling users to consume content, with only a few of them also producing it [2].

The second stage was represented by Web 2.0, fueled by the growth of social networks, increase in user-generated content and user interaction and collaboration [4]. Still, Web 2.0 is commonly associated with a centralised hierarchy, where big tech corporations owned the major platforms where users can produce and consume content [4]. This stage coincided with the Dot-com bubble, as excessive speculation of Internet companies led to a sudden crash in the stock markets in early 2000s [5]. Eventually, the industry managed to surpass this turning point and the Internet became a common tool for the majority of the world population [6].

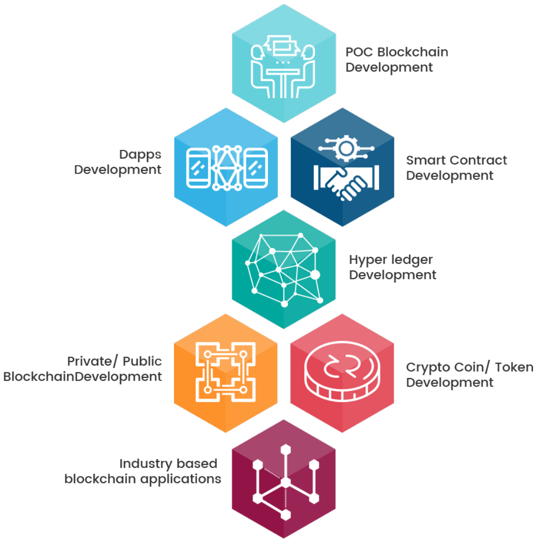

POC Blockchain Development
Dapps Development
Smart Contract Development
Hyper ledger Development
Private/ Public BlockchainDevelopment
Crypto Coin/ Token Development
Industry based blockchain applications

Figure 1.1: Blockchain Use Cases. Source: [3]

There is however a new vision for the future of the Internet that aims to decentralise the World Wide Web, to empower users and to democratise access by taking away the power from large corporations [7]. This vision is represented by Web3, a term conceived by Ethereum co-founder Gavin Wood [8]. Years after Bitcoin's emergence, the meaning of decentralisation has expanded towards the possibility to build decentralised applications (dApps) that serve various areas, such as finance, supply chains, energy and even art [9].

As mentioned, art is one of the domains that has witnessed the disruption created by the emergence of blockchain technology, that continues to happen even during at the time of writing [10]. The enablers of this disruption are the Non-Fungible Tokens (NFTs), digital assets characterised by uniqueness and hence, that cannot be substituted and that are tradeable on the blockchain [10]. The stored data also includes the hash of the linked asset and ownership history, fact that enables transparency in the value of the asset being traded.

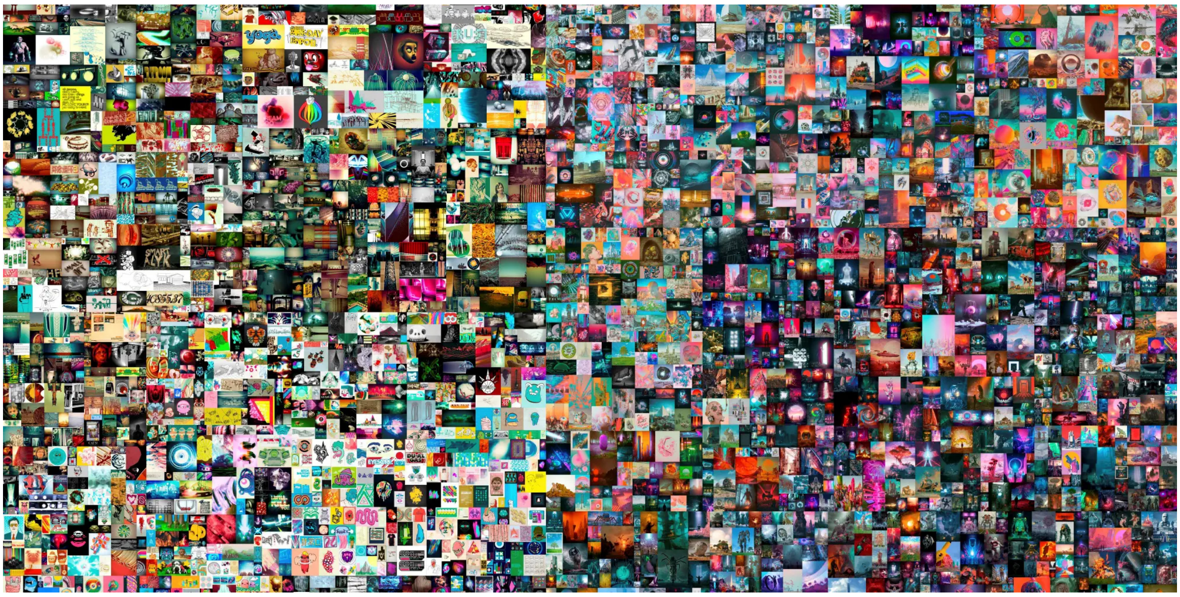


Figure 1.2: ‘Everydays: the First 5000 Days’ NFT by US-based artist Beeple

The similarity between a digital token and an actual art piece is that both of them are unique and hence, their value is also given by scarcity [10]. While an NFT can be tied to a specific physical artwork, it is often the case where NFTs are only representing digital assets such as digital artwork, music or videos.

Having a high traction and increased demand, assets such as the very first tweet produced by Twitter co-founder Jack Dorsey, a top shot of American basketball player LeBron James scoring for LA Lakers or a collection of ape illlustrations were all sold on various marketplaces for millions of US dollars [11, 12, 13]. With an immense adoption speed, the phenomenon gathered much controversy, as claims state that the intrinsic value of NFTs only stands in the hype created and the speculation attributed to that, some being afraid that this might even lead to a second Dotcom-like bubble [14].

Several blockchain enthusiasts argue about the value created by NFTs [15], while some righteously question the authenticity of these assets, especially based on the current lack of regulation that is governing the blockchain and NFT area [16]. While blockchain indeed stores a record of the ownership tree and the value that was paid for an NFT at a given point in time, it is still unclear how can an NFT be verified for authenticity, given the fact that it is first publicly visible (and downloadable) and the initial seller of an asset is also able to claim ownership of the tied media file, if nobody else does it or if the statement is not contested. To back these hypotheses, OpenSea - one of the largest digital NFT marketplaces, admitted that more than 80% of the NFTs they were hosting were fraud or plagiarised [17]. Further, there have been several cases where buyers were lured into purchasing forged NFTs, such the case of a fake Banksy (street artist) artwork being sold for GBP 244 000 [18] or the 'Evolved Apes' NFT developers who vanished a week after launching the project and earning 798 ETH (USD 2 250 800 at the time of writing) [19].

Regardless of this, the industry is is here to stay, as it is still in its infancy and is gaining continuous traction. According to Citi Ventures, 'NFTs are the building blocks of the Metaverse' [20], the even newer technology that powers virtual worlds where users socialise, meet and play [21]. Artists are more eager to step into the digital ecosystem and investors are more interested in the evolution of technology and even the transition from traditional art towards digital art [10].

NFTs still represent a risky asset, not only from the perspective of market volatility but also for the transparency in the actual origin of an artwork. This is the reason why the industry of digital collectibles needs to be enhanced, for the benefit of both artists and investors who should be able to safely and securely be able to trade artwork online, with a minimal risk factor and by being protected from fraudulent activities and counterfeiting.

1.1 | Research Question

How can blockchain technology aid in certifying the authenticity of NFT digital artwork so that art investors can trust the value of their investment?

1.1.1 | Sub-Questions

1. How can decentralisation, in general, contribute to a more secure environment for trading digital collectibles?
2. How can a decentralised authentication mechanism assist in preventing fraudulent activities and counterfeiting within the NFT industry?
3. How should NFT marketplaces be held liable for the user-generated content (i.e. NFTs) stored and traded within the platforms?

1.2 | Delimitations

For being able to obtain unprejudiced and veracious findings, listing the delimitations that are set for the trajectory of the current research is an essential duty. As such, it is imperiously necessary to narrow the scope of the project to focusing on the blockchain and cryptography-related aspects of what such a solution would involve. By doing so, an in-depth perspective can be formed and other side tracks that the solution could have a prospensity for, would be obsoleted. Such cases include considering technologies different than blockchain as being the main enablers behind an eventual solution. However, this is not to discard other technologies that could potentially aid in achieving the purpose, but simply to demonstrate the blockchain's capabilities in regards to the illustrated matter.

Besides this, blockchain and especially the NFT ecosystem are still niche areas, as according to consumer data company Statista, less than 4% of the global population has had any contact with the technology in 2021 [22], given a global population of 7.9 billion. As such, another preset delimitation is to collect primary data mostly from sources and subjects who at least have a minimal knowledge or have had some experience within the ecosystem. In this regards, it is possible to include survey and interview respondents, and the purpose is to obtain valuable insight that can reliably be used in the course of the project.

1.3 | Key Terms

1. *Blockchain*: A decentralised and distributed database, controlled by no single authority, that stores data in the shape of blocks that are chained using advanced cryptographic functions [23].
2. *Non-Fungible Token*: A unique unit of data stored on a Decentralised Ledger that is usually associated with digital media files [24].
3. *Fungibility*: The ability of a good or asset to be interchanged with other assets of the same type [25].
4. *Digital Art*: Art that is made or presented using digital technology [26].

1.4 | Thesis Structure

The current thesis is following a concise structure, described in the paragraphs below.

The *Methodology* section illustrates an array of methods and theoretical frameworks used throughout the thesis. Among them, the process model of choice is described, the primary and secondary data collection techniques and the testing framework, that includes both software testing and user/usability testing.

The *State of the Art* section initiates with a comprehensive *Literature Review*, where existing research papers and academic theses are described for being able to identify the gaps existing in the current knowledge on the NFTs ecosystem. Further, *Technological Enablers* that are going to be used in the development of a functional prototype are described, continued by a thorough analysis of existing marketplaces as *Case Studies*.

The subsequent section illustrates the findings from the *Expert Interviews* and the *User Survey*, while the next one encompasses the *System Requirements Engineering* process, that uses the entire array of findings as its foundation. The process consists of identifying personas, developing user scenarios and use case diagrams, eventually being concluded by the functional and non-functional requirements specification.

Subsequently, the *Technical Implementation and Evaluation* comes next, where the whole concept and system architecture of the functional prototype are described. Besides that, the section includes an overview of the used frameworks and libraries and a thorough technical description of the most relevant developed features. Then, the *Testing* section elaborates on the performed software tests, user and usability tests and the *Requirements Validation* subsection that naturally derives from it.

The *Discussion* section elaborates on how the solution and findings relate to the empirical data collected throughout the previous sections and also provide an overview of the limitations that affected the course of the project.

Eventually, the *Conclusion* provides answers to the stated research question and sub-questions, being followed by a list of further improvements that could possibly be included in the backlog of a future iteration on the prototype, and also by a brief description of how the current work brings value to the academic knowledge about the blockchain and NFT ecosystem.

2 Methodology

To every problem, there is a most simple solution.

Agatha Christie, The Clocks

2.1 | Project Scope and Description

Among the several innovations powered by Blockchain technology, NFTs or Non-Fungible Tokens are one of the newest of them. They are defined as unique units of data stored on a DLT that are usually associated with digital media files and they are already being transacted on specialised platforms for thousands or millions of dollars [24].

With such a high speed of adoption rate, the industry lacks regulation at the time of writing [16]. Consequently, besides the opportunities that NFTs enable both for art creators and buyers/investors, the area is highly susceptible to fraudulent activity and counterfeiting [27].

Therefore, the scope of the current project is to investigate how can NFT technology be enhanced for certifying the authenticity of digital artwork, so that art investors can trust the value of their investment. For answering the problem formulation, a thorough research will be carried, consisting of primary and secondary data collection, as well as a State of the Art section where existing NFT marketplaces will be analysed as case studies.

This would eventually converge into building a solution to the stated problem in the shape of a functional prototype that would include both minting and trading an NFT while considering the fraud prevention mechanisms that would be developed.

Eventually, the system would be tested and further iterations for its development would be considered, for refining and enhancing the given solution.

2.2 | Software Process Model

At this early stage, it is imperiously necessary to adhere to a software process model scheme aimed to ensure a solid path and the workflow plan of such a project. Besides this, even if the entire workload is assigned only to a single author, there is still a need to adopt it, since it is truly important to ensure that each step is acknowledged, handled and delivered efficiently within the proposed time interval by achieving the desired results.

A software process model alludes to a detailed and elaborated set of activities and stages for specifying, designing, implementing and testing the solution [28]. Therefore, an intensive analysis of a vast range of potential models lead to an agile methodology adoption, as this decision would be the most suitable process model to enhance software efficiency.

More specifically, the SCRUM framework would be used due to its well recognised characteristics. Also as Schwaber K. and Sutherland J. confirmed, SCRUM and its self organising procedure of using a framework based on an iterative, incremental approach seems to increase the potential predictability in regards to project success while risk being diminished [29].

Needless to say that, in this context such a model complements the organisational aspect of the project as the SCRUM model is widely used in small teams, facilitating a high degree of flexibility in implementation in an agile fashion [28].

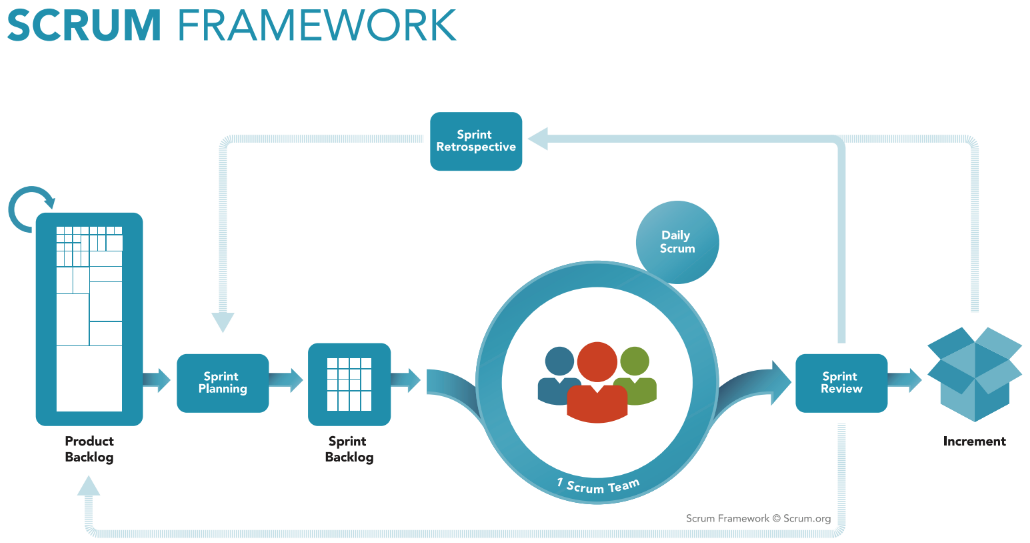


Figure 2.1: SCRUM Framework. Source: [30]

2.3 | Data Collection Techniques

In order to collect reliable and comprehensive data to base this study upon, it is necessary to conduct a thorough research within the blockchain ecosystem and more specifically, the NFT industry.

Therefore, in the manner of counterbalancing potential weaknesses carried by the use of a single type of data collection method, mixed methods of gathering data would be used. The primary and secondary data collection techniques are extremely valuable tools for creating a solid foundation for the current project.

As the primary objective of the thesis is highly concentrated on the value creation and also, since the validity of the findings is highly significant, there is no doubt that empirical documentation must originate from trustworthy resources.

Thus, the secondary data consists of information that would be collected and quoted from scientific papers and research articles, all originating from reliable and trusted publications and entities, such as universities, research centres or consulting firms (eg. PwC, EY, Accenture). Nevertheless, even if scientific literature and books have a major contribution within the process, the novelty factor of blockchain and NFT technology causes a limited amount of scientific resources. For this reason, alternative data sources, also originating from reputable entities, will be used. Among them, it is possible to count international organisations (eg. World Economic Forum - WEF) or alternative media outlets (Vice Media, Reuters, Time Magazine).

When considering collecting primary data for the purpose of the current thesis, both quantitative and qualitative techniques would be used. The creation and distribution of a user survey represents the quantitative type of study and would elicit accurate and meaningful feedback from the potential users of the solution to be developed [31]. Besides this, the results would later be used in this project, serving as a genuine foundation in decision-making process establishing the requirements for the solution to follow.

Besides this, a qualitative type of study would complement and strength the findings by learning from experts' insights. Therefore, expert interviews are considered to be conducted within this project for acquiring a more critical perspective and therefore having an extensive understanding into the experts field [31]. By doing so, it will allow for an unbiased perspective over defining a solution that would both fulfil consumer needs and also fit into the technical framework that experts would advise for.

2.4 | Design Thinking Process

The design thinking ideology revolves around iterative and incremental approaches of identifying and tackling ambiguous factors that might interfere with the problem-solving process [32]. This methodology attempts to constantly improve findings until the innovative desired solution is achieved.

Moreover, at the heart of Design Thinking stands the user-centric approach for problem solving. This can be described as a collection of practices and methods of analysing how a prospective user would interact with a system, in order to acquire realistic and factual user needs and expectations [32]. Therefore, the creative element of Design Thinking establishes methods that can further reveal multiple avenues for problem tackling.

Accordingly, it is certainly essential to integrate a design process model within such a context due to the aforementioned benefits. With such a complex and innovative system under development, the 5-Stage Model of the Design Thinking Process will be be a relevant model to adhere to.

The 5-Stage model was established by Hasso-Plattner Institute of Design at Stanford and it focuses on a non-linear process following an overall flow of 5 specific stages [33]. Consequently, as it can be seen in figure 2.2, every step describes a systematic set of action points within the process, that can be iterated without following any specific order [33].

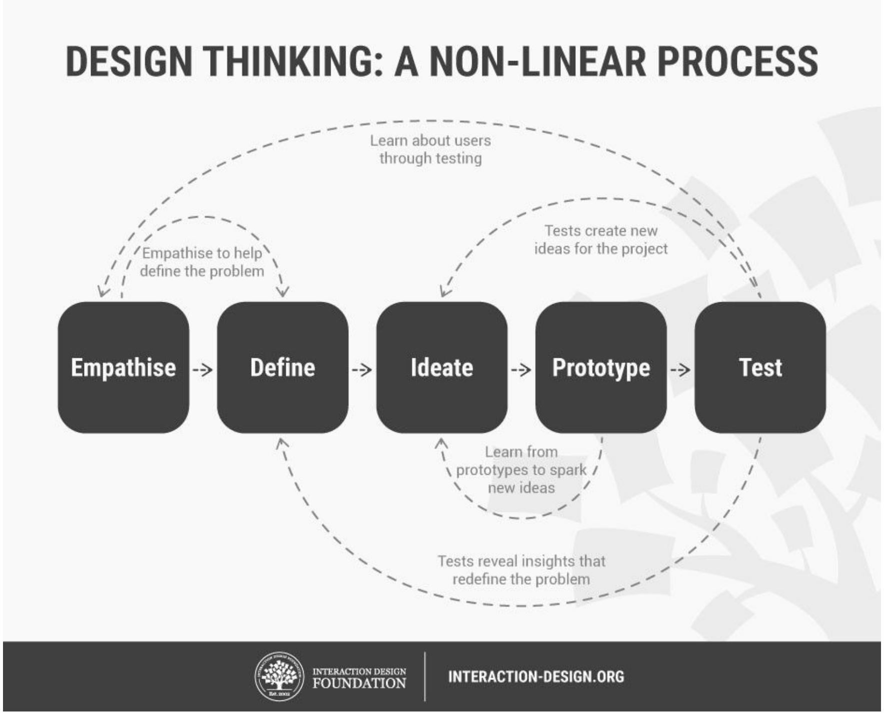

DESIGN THINKING: A NON-LINEAR PROCESS
Learn about users through testing
Empathise to help define the problem
Tests create new ideas for the project
Empathise
Define
Ideate
Prototype
Test
Learn from prototypes to spark new ideas
Tests reveal insights that redefine the problem
INTERACTION DESIGN FOUNDATION
INTERACTION-DESIGN.ORG

Figure 2.2: Design Thinking Process. Source: [33]

To proceed, the ‘Emphatise’ step, as the name suggests, refers to the actual research conducted to gather insights about the prospective users’ expectations and perspectives, in regards to the potential solution [34]. The method used to develop an understanding of the users, mainly based on user surveys, followed then by expert interviews, which represent another method used to strengthen the findings and to collect empirical data from expert insights.

The ‘Define’ stage exploits data gathered in the ‘Emphatise’ step, by merging all the observations and narrowing them down in the shape of the problem statement [34]. Within this step, personas can already be depicted as fictional characters representing specific user segments. User scenarios are also created and they serve as a solid pillar for designing a set of UML diagrams, more specifically the Use Case Diagrams.

Another significant step alludes to the ‘Ideation’ process. At this point, by reflecting on the research done in the ‘Emphatise’ step and by also re-iterating the ‘Define’ step results in a brainstorming session that would be eminently helpful for giving the solution a concrete direction [33]. In this phase, a set of functional and non-functional requirements are engineered.

The ‘Prototype’ stage is one of the most important parts of design thinking. As Milton Glaser (renown American graphic designer) preaches, *‘It’s about taking an idea in your head, and transforming that idea into something real. And that’s always going to be a long and difficult process’* [33]. The takeaway from here is that during this stage, the solution is going to be materialised. Within this step, the actual implementation process, including the development of the solution in the shape of an MVP (Minimum Viable Product) is carried out.

Eventually, the ‘Testing’ stage can accurately assess if the solution can be validated, by simply returning to the users for important feedback [33]. This phase covers processes such as continuing the user research by involving them and conducting usability tests based on the functional prototype [33]. By acknowledging users’ feedback, new or improved features could be added to the backlog for scaling the existing solution in the upcoming iterations.

The outcome of the 5 stage model mentioned above represents the backbone of a solid process intended to align the entire array of phases, aimed to ensure the focus for achieving the desired solution [33].

2.5 | Testing Framework

As an extension to the ‘Testing’ stage of the Design Thinking Process, testing should start within the functional prototype by running unit, integration or system tests, depending on the prototype’s nature and requirements. Besides this, usability tests are considered, in order to obtain direct user feedback on the solution that will serve as the starting point for the next iteration of the product. Based on software and usability tests on the functional prototype, it is possible to assess the state of implementation of the requirements to be defined. In other words, the requirements validation process is one of the direct outcomes of the testing phase.

2.6 | Hypotheses and Assumptions

One of the core hypotheses derived from the resources mentioned above consists in the fact that even if terms as blockchain, NFTs or smart contracts are novel concepts and still in the incipient phase, both art creators and consumers are eager to adhere to such new technologies in the detriment of solely relying on the traditional art ecosystem.

Moreover, it seems that most of the people interested in NFT technology and digital art are visibly more incentivised by the blockchain properties claiming for transparency or security, that can lead towards an efficient adoption of dematerialised artwork.

On the other hand, another assumption worth mentioning is that there is still a need for a regulatory framework around the NFT industry, for providing an increased level of trust among the digital art enthusiasts. With regulations in place, NFT marketplaces would become a safer place to trade digital art and collectibles, both for art creators and consumers.

The statements mentioned above would be further elaborated and validated in strong correlation with the collected data, by the time the research question finds its answers in the conclusion of the thesis.

3 State of the Art

The current section aims to research and discuss the currently available scientific knowledge and practical solutions, their strengths, drawbacks and their underlying technologies. Thus, the ‘State of the Art’ helps in defining a clear picture of the entire mechanism behind existing similar solutions [35] and extrapolates over what is missing within the current NFT ecosystem. With this newly collected data, it is possible to define a more clear objective for the solution that will be proposed in the course of this thesis.

For the purpose of consolidating a solid research, the first subsection introduces and reflects upon literature review that would further assist in documenting and in the decision making process, later within the thesis. Therefore, this very first step bridges towards the most relevant case studies that would be selected and analysed further. This part aims to focus on a comprehensive analysis of similar existing solutions, that would also include an overview into the systems’ technical implementation and limitations.

Apart from this, the State of the Art also includes a subsection dedicated to the technological enablers that power the industry, for obtaining an understanding of the underlying technologies and a direction for the practical aspect of building a working prototype, in the scope of a MVP. The ultimate part of this section would support a summary of essential findings. All the valuable information gathered within this section, through a prism of strong observations and understandings, would contribute to offering a clearer direction into both the primary data collection methods that will follow and the evolution of the working prototype to be developed.

3.1 | Literature Review

Several studies indicate that digital art has recently recorded an impressive social impact, driven by both the advanced pace that the blockchain industry develops, and also by the widespread media coverage and mainstream adoption [10, 19]. However, the novelty factor also brings skepticism and raises distinct questions when it comes to how valuable and secure NFTs are. In other words, there is an ongoing debate in the academic environment and also in the blockchain ecosystem on the value that NFTs deliver and on the authenticity of the related artworks.

Accordingly, this section aims to draw attention to the appropriate raised questions and to parse a thorough and comprehensive literature review on blockchain-based digital collectibles. Consequently, the primary interest for the section is to concentrate around the divergent opinions stated in scientific research papers and to highlight the gaps that exist and that will be covered in the current thesis.

3.1.1 | Process

Conducting a thorough literature review involved an array of processes that needed to be carried systematically. For finding relevant research papers, theses and articles it was necessary to establish a set of scientific databases that would be browsed. Among the most relevant ones, it is possible to count libraries such as JSTOR, IEEE Xplore, ACM Digital Library and Google Scholar.

The next step was to align on the key words that would be used. Consequently, the search was initiated with terms such as ‘NFT’ or ‘blockchain’, but it was rapidly refined and focused for more specificity. One way was to join the terms, such as ‘NFT blockchain’ and to add up more ‘NFT blockchain security’, ‘NFT authenticity’, ‘digital art blockchain’.

The selection of articles was based on the degree of relevance to the topic, the number of citations (denoting a more trustworthy source), the publishing institution and the quality of the references specified within the paper. Also, there was a focus on preserving different angles over the shortcomings or benefits that the NFT industry brings, so papers with diverging outcomes were considered, with respect to the aforementioned criteria.

3.1.2 | Analysis and Findings

From a chronological perspective, the first relevant article from the researched list was published in 2017, before the term NFT was popularised. The paper is called *Visibility and digital art: blockchain as an ownership layer on the internet*, co-authored by blockchain professionals McConaghy M., McMullen G. et al, and by Bristol Business School professor Parry G [36]. In a brief, the paper discusses how blockchain technology can facilitate the transparency for ownership chains within digital art, with holding specific metadata on digital property [36].

The authors discuss the need for a better visibility in the information flow related to digital assets, as information asymmetry can often lead towards conflicts of interest [36]. This translates to the ability for a user to request an image from a server, to view it and download it, leaving the author of the image without any possibility of knowing how is the image consumed and used further.

Further, the Bitcoin blockchain is considered as 'a part of the potential solution', for the purpose of being used as a decentralised storage for the transactions of digital assets/art, storing metadata such as attribution, transfers and a provenance chain for each asset [36]. While the paper dives into copyright and intellectual property aspects, it is worth mentioning that NFTs in the current shape do not pertain copyrights or intellectual property with the proof of ownership [10].

However, aspects such as provenance are clearly defined, as this term encompasses the biography of a digital artwork, proof of authenticity and attribution [36]. Another relevant aspect discussed was using AI and web crawlers for tracking occurrences of digital artwork and their copies online, which allows artists and creators to spot copyright infringement and to be able to address them [36].

One of the key takeaways from this paper is that the copyright and Intellectual Property Rights (IPR) issue is a different aspect from the NFT ownership structure, but a similar approach should be considered for the current case. However, while the focus is mostly on helping the creators by limiting the amount of piracy and copyright infringement, there is little to no input on consumers' protection from the risk of purchasing unauthentic or counterfeit artworks, as the ownership chain begins with the initial publisher of the asset, who might as well not actually be the actual author of the artwork.

At the other end of the spectrum stands a research article published by Springer in the *Philosophy & Technology* journal in 2016. Zeilinger M. argues in his paper, *Digital Art as 'Monetised Graphics': Enforcing Intellectual Property on the Blockchain* that the attempt to add artworks to the digital world by using blockchain technology has as a direct effect the transformation of art into nothing more than just a commodity based on artificially created scarcity [37].

Hence, Zeilinger claims that this can also lead to hindering the artists' ability to own and manage their creative work, and also to limit the artistic expression with a 'financialised' approach over the produced assets [37].

Further, one of the more recent research papers eventually introduces the term NFTs that brings a more moderate perspective over the perceived value and scarcity that surrounds them. The paper is 'Non-Fungible Tokens: Blockchains, Scarcity, and Value' by Chohan U.W. and it correlates the inherent scarcity given by the NFT's non-fungible nature to the perceived value, mapped to the economic correlation between supply and demand [38].

Also as a mean of allowing artists to monetise their work, the author presents a brief example of music history where platforms like Spotify enabled a new way of monetising music [38], without though reducing the risk of online piracy. Likewise, NFT technology can contribute to monetising art (either music, paintings, illustrations, etc.) but not necessarily to reducing the amount of theft or counterfeiting that is happening in the industry [38].

The author concludes that the value of NFT units is directly proportional to the amount that buyers/investors are willing to pay. Also, with the ownership aspect being represented by only a hashed reference to the asset that is stored in a crypto wallet, that reference can lead to a non-existent item, in the case that it has been relocated, deliberately or not [38]. Consequently, there is a risk of cyber theft or hacking attempts that is yet to be mitigated by blockchain technology [38].

Further, another paper that analyses, among others, security aspects and related challenges that the NFT industry currently faces is 'Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges' - a technical report authored by researchers from the University of Birmingham and Swinburne University of Technology [10].

The report also includes a technical description of the underlying layers of NFT technology, that will be referenced in the technical analysis subsection of the State of the Art (3.2). However, information that is relevant for the scope of the current literature review relates more towards the security evaluation carried in the report and the related challenges.

For assessing the security parameters, the authors use the STRIDE threat and risk evaluation model developed at Microsoft in 1999 [39]. STRIDE is an acronym for six categories of security threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DoS) and Elevation of Privilege [10], each of them being addressed with certain recommendations for mitigating the risk.

Spoofing refers to impersonating other actors in a system, which breaches the authenticity security parameter [10]. Spoofing can be performed by gaining access to users' private keys, which can lead to NFTs and other crypto assets from the users' wallet being transferred irreversibly in the attacker's wallet [10]. For mitigating this risk, the authors recommend using cold wallets for storing NFT assets [10]. Furthermore, *Tampering* means modifying the underlying data of an NFT and hence, violating the integrity security parameter [10]. This is a risk to any data stored outside the DLT, so it is also recommended to send the original data besides the hash of the asset when performing a transaction [10].

Among the enumerated challenges, the authors emphasise the trade-offs between anonymity and the legal pitfalls that the NFT industry is currently facing. The concerning areas are the partial privacy given by the Ethereum network joined by the poor and outdated regulatory frameworks in several jurisdictions that are not adapted to the current state of the blockchain industry [10].

3.1.3 | Summary

From the selected research articles mentioned above, it is possible to derive that even if NFTs do not involve transfer of IPR or copyright, there is still a need for increased transparency over the information flow, so that digital art creators can trace their artworks after being traded. Besides this, the scarcity that NFTs imply is a leading factor in the current market condition and such an investment should involve considering several other aspects. One of them is the source of the artwork, which should be trusted to be the initial poster of the asset on a marketplace, but is this information enough for the buyers to trust?

This question relates directly to what the quoted articles are missing, which is the risk of illicit activities that can occur due to the lack of regulation within the market. The risk factor is shared by both digital art investors and creators, as creators are likely to have their work stolen and offered as original content on similar NFT platforms, while investors risk purchasing counterfeit NFTs that have no inherent value (as in the case of the Banksy artwork counterfeit [18]).

Apart from this, other associated risks are malicious actors involved in tax evasion or even money laundering schemes who can take advantage of the anonymity associated with crypto wallets and place the illegitimate funds into digital artworks or even other assets, such as Tweets being traded as NFTs.

Consequently, it is possible to conclude that there is a gap in the current research in terms of NFT technology being able to acknowledge the real author of an artwork. This is also reflected in the case studies being showcased in the State of the Art section, with OpenSea openly admitting that a majority of the content hosted on their platform represents counterfeit, as previously specified [17]. Therefore, one significant finding is that while blockchain and more specifically NFT technology represent a secure way to store immutable data on such transactions, the way the market currently operates on the assumption that the original poster of an NFT on an online marketplace is actually the creator of the asset, can lead to presenting inaccurate or unrealistic information that can cause considerable financial loss for involved parties.

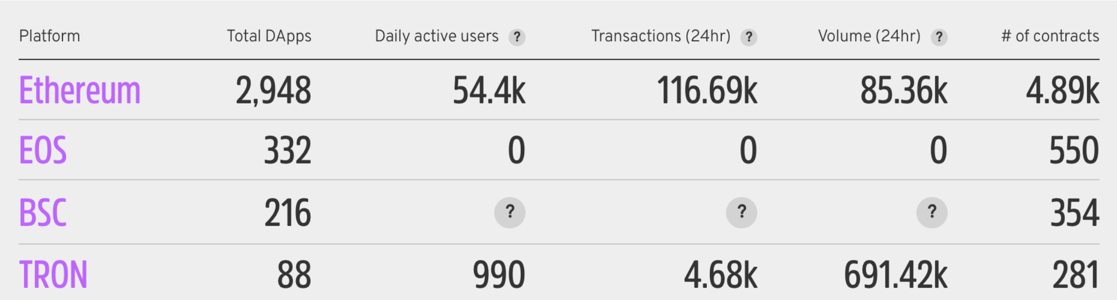
3.2 | Technological Enablers

The current subsection aims to investigate and analyse the underlying technology behind NFT, for obtaining a clear picture of how do they work and what makes them so disruptive. Consequently, the current subsection leads to an understanding of the technicalities, such as supporting networks, standards and ways of storing content.

3.2.1 | NFT Networks

Among the several different blockchains that were established after Bitcoin's release, it is possible to focus on those that were initially set to power dApps, as many of them have recently evolved to support holding and trading of NFTs, besides their native cryptocurrencies.

One of the most relevant networks to analyse is Ethereum, an open and permisionless blockchain that powers the majority of the current dApps across the Internet, as seen in figure 3.1 [40]. The main feature that Ethereum comes with is the support for smart contracts written in Solidity, an Object-Oriented Programming language similar to Javascript [41] that allows Web3 developers to create seamless interaction between the built dApps and the Ethereum blockchain.



Platform	Total DApps	Daily active users ?	Transactions (24hr) ?	Volume (24hr) ?	# of contracts
Ethereum	2,948	54.4k	116.69k	85.36k	4.89k
EOS	332	0	0	0	550
BSC	216	?	?	?	354
TRON	88	990	4.68k	691.42k	281

Figure 3.1: Top platforms used by DApps. Source: [40]

While Ethereum is a public and permissionless blockchain, participation is only limited by using a crypto wallet and transactions are only tied to the wallet addresses, which are nothing more than random strings of hashed values for identifying a wallet [42]. While all the transactions are visible and public on the Ethereum network, user privacy is not affected due to the aforementioned reason [42]. Further, each transaction has an associated fee which is paid by the issuer in *gas*, for preventing spam and misusing the network [42].

One key factor about the Ethereum blockchain is that it currently uses the Proof of Work (PoW) consensus mechanism for validating transactions, which is an algorithm that uses heavy computational resources where validator nodes compete against each other for solving complex mathematical problems [43]. Also called crypto mining, it represents a highly controversial topic in the environmentalists sphere, as the activity is reportedly consuming enormous amounts of energy - Bitcoin yearly averages are comparable to the consumption rates of Austria or Norway [44]. Besides this, with the steep increase in popularity and an often congested network, gas fees have sharply increased, making most of the small sized transactions worthless [45].

However, Ethereum is in the transition process to the Proof of Stake (PoS) mechanism [42], which has far less impact on energy usage and the environment, as transactions are being validated by nodes according to their staked amount in the corresponding cryptocurrency that powers the Blockchain [42] (in the current case, Ether - ETH). With a perspective to fully transition towards PoS by the end of 2022, it is not possible to assess whether that will actually be the case, since the estimation has already been postponed two times before [46].

Another blockchain that recently started to gain more recognition and that aims to solve some of the inherent drawbacks of Ethereum is Polygon, previously known as Matic [47]. With a PoS protocol already in place, Polygon is a Layer 2 blockchain (extending Ethereum and built upon it [42]) that is focused on enhanced scalability and reduced associated transaction fees [47].

Due to this, Ethereum functionalities are also preserved in the Polygon chain, so features such as Solidity smart contracts and other tools are still a viable solution for using on Polygon [47]. Besides this, another software quality attribute that Polygon satisfies is interoperability, as with Polygon Bridge it is possible, for example, to transfer ETH from the Ethereum network to Polygon seamlessly, and the other way around [48].

Being powered by MATIC, its native cryptocurrency, Polygon also claims to offer high performance denoted by a throughput rate of 10000 transactions per second (TPS) [48].

From an architectural perspective, the Polygon network uses three different layers: the Ethereum layer, that features a set of smart contracts on the Ethereum mainnet, the Heimdall layer that is mainly used for the actual PoS validation process and the Bor layer aggregating transactions into blocks that are pushed to the Heimdall layer for handling them into a Merkle tree [48].

For the benchmarking purpose, both networks are viable options for the functional prototype to follow, as Ethereum features an extensive documentation and discussion in development forums (i.e. Stackoverflow), while the newer Polygon network brings with it performance and cost-related benefits, as mentioned above [48].

3.2.2 | NFT Standards

One of the most used token standard used in regular smart contracts is the well known ERC-20, which is mapped to fungible tokens of any nature: fiat currencies, votes, ounces of gold, etc. [42]. What all of these have in common is their fungibility, as a token representing an ounce of gold can be traded for another one that represents an identical ounce.

For this reason, there was a need for a different standard for non-fungible assets, and the most relevant ones is the ERC-721, a standard proposed in January 2018 that defines an API interface for Solidity smart contracts [49]. The interface specifies the uniqueness of the token it represents, which is given by properties like age, rarity or the visual element that it is mapped to [50].

A smart contract has to implement functionality like 'minting' new tokens (creating an NFT), transferring them between accounts, getting the token balance and the total supply of the token that is available on the network, in order to be compliant to the ERC-721 standard [50]. Other key functionalities include approving the transfer of specific amounts of a token by a third party account [50]. The proposal of the ERC-721 standard states that each NFT uses a unique `uint256` identifier inside a smart contract, which shall not change during the lifetime of the contract [51]. Also the asset is highly dependant on the contract address that generates it, so that the pair between the contract address and the token ID represents a 'fully-qualified identifier' for the asset [51].

Further, there is also the ERC-1155 standard, which is an interface for contracts that is able to manage fungible, non-fungible and even other configurations such as semi-fungible tokens [52]. According to the official documentation, it improves both the ERC-20 and ERC-721 standards, as it is more efficient and it corrects some inherent implementation errors [52]. However, even if the standard was released only six months after ERC-721 and it is already an official Ethereum standard [52], the adoption rate is slower and there are less resources referring to it in the Web3 developer community.

3.2.3 | Content Storage

As previously stated, a main difference between a fungible and a non-fungible token is is that the latter also has a file attached to it, in the shape of a URL leading to it. Accordingly, there are two sides related to storing an NFT, which are the storage of the private key that holds the hash code and the storage of the actual underlying asset or media file [53].

While the NFT hash is stored on the ledger in an immutable and tamper-proof manner, it is almost impossible to store the associated media file and its metadata on-chain, primarily due to scalability issues [53]. For this reason, there are two main storage solutions: the classic centralised cloud-based option and the decentralised approach, each of them coming with their own set of benefits and drawbacks [53].

An advantage of centralised storage is that it is a fairly straightforward process to use, as any basic cloud server configuration can support uploaded files of selected MIME types and formats. Some of the well known services are AWS S3 (Simple Storage Service), AWS EFS (Elastic File System), Azure Files or Google Cloud Filestore.

However, this comes at the cost of centralisation, which employs a single point of failure and still, keeping the power in the hands of a single actor [54]. Moreover, the file metadata is also stored in a centralised fashion, which makes it susceptible to being tampered with [53]. In such a scenario, the hash value of the NFT stored in an user's crypto wallet would permanently lose the reference to the altered asset, leaving the user with an NFT pointing to an empty source with no left value on it. Further, it is also possible that the server shuts down, has outage issues or even that the custodian of the files interrupts the contract with the cloud provider and removes the files from the cloud storage. Any of these actions would lead to same output, which is leaving the actual owner of the NFT with an empty reference in the hash key stored on their wallet.

To address the issue, alternative methods have been developed and one of them is the IPFS protocol, which is an acronym for the InterPlanetary File System [55]. According to the official documentation, IPFS is a distributed storage network that can handle data such as files, applications or even websites [55].

While a HTTPS connection to a centralised server is performed by querying its physical location, a native IPFS connection with an URL shape of `ipfs://{contentId}/path/to/resource.jpg` is querying the resource by its content [55]. As the network is distributed, there are likely several peers that are serving the accessed content instead of a single server. With such an architecture in place, IPFS can lead to a more resilient and less censorship-prone internet, according to the documentation [55].

It is therefore natural to fit NFT files and their metadata in this framework, since the decentralisation of the file storage layer leads to an immutable and tamper-proof manner for storing them [53]. Files stored on IPFS also feature a cryptographic signature of the issuer and a Content ID (CID) that represents a set of hashes based on the file's location and metadata [53]. The Content ID is where the NFT's hash value stored on the users' wallet can point to [53].

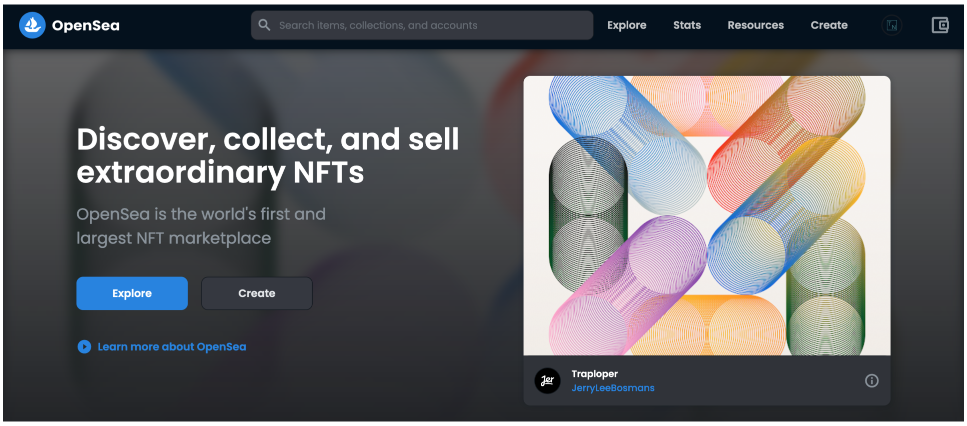
However, decentralised storage options as IPFS come with their own limitations. For example, if an arbitrary file that was initially released on the IPFS network by a certain actor is not being downloaded and hosted by other nodes, this method becomes as vulnerable as the centralised server approach, as there is no more than a single entity serving the file [56]. Accordingly, there always needs to be at least one active node that can serve a file in order for it to be available to the rest of the network. Even so, the resilience and 'anti-censorship' benefits evoked by the creators of IPFS might not outperform those of a centralised server, but at minimum the immutability of the file metadata remains in place [53].

Nevertheless, with enough available nodes that serve the assets, IPFS can leverage its key resources and the purpose of storing immutable and tamper-proof NFT files and their corresponding metadata can be successfully achieved.

3.3 | Case Studies

The following section consists of analysing a set of case studies representing digital NFT marketplaces that had a large market share at the time of writing. Following similar principles as in the case of the Literature review conducted above (section 3.1), the search carried on different search engines included terms as ‘digital art’ and ‘NFT marketplace’. The selected options have been chosen both due to their popularity in the crypto ecosystem, as well as for highlighting the different approaches and underlying supporting technologies that they featured.

3.3.1 | OpenSea



Discover, collect, and sell extraordinary NFTs

OpenSea is the world's first and largest NFT marketplace

Figure 3.2: OpenSea Platform. Source: [57]

OpenSea is by far the largest NFT marketplace by sales volume, as displayed by figure 3.3. The company was founded in 2017 and and has experienced enormous growth since the beginning of 2021, with the increased general interest in the NFT space [58].

In terms of blockchain networks and cryptocurrencies, OpenSea supports Ethereum, Polygon, Klaytn and Solana, with the last one being in Beta at the time of writing [57]. Also the core currencies that are accepted are ETH, SOL (Solana’s native currency), USDC (stablecoin pegged at the value of the USD) and DAI [57]. Access to trading NFTs is only limited by connecting a browser wallet such as MetaMask to the platform, allowing the users to either purchase or mint and expose their assets in the marketplace.

Further, OpenSea recently transitioned from centralised storage of the files and their metadata towards a decentralised system powered by IPFS and Filecoin [59]. While this is an important step towards building a more resilient architecture, it is currently an optional feature that creators can choose when minting their NFTs.

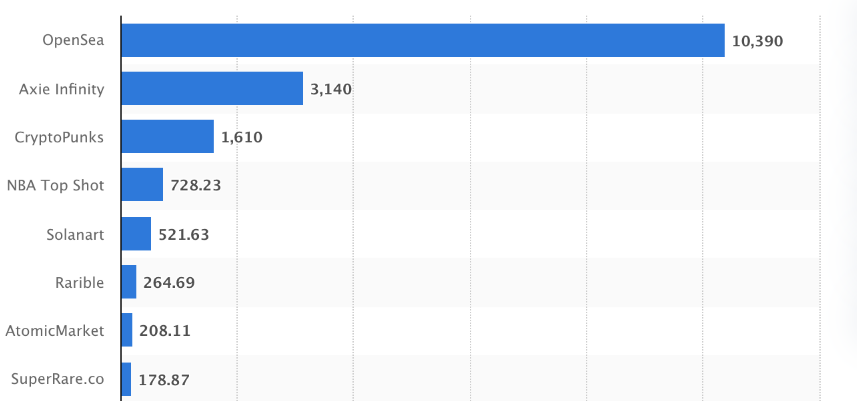


Figure 3.3: Largest NFT marketplaces based on all-time sales volume as of November 11, 2021. Source: [60]

Even with the strengths mentioned above, OpenSea has often been the subject of controversy among the crypto community [17]. As previously stated, the company representatives openly admitted that up to 80% of the NFTs they host on their platform are counterfeit or plagiarised [61].

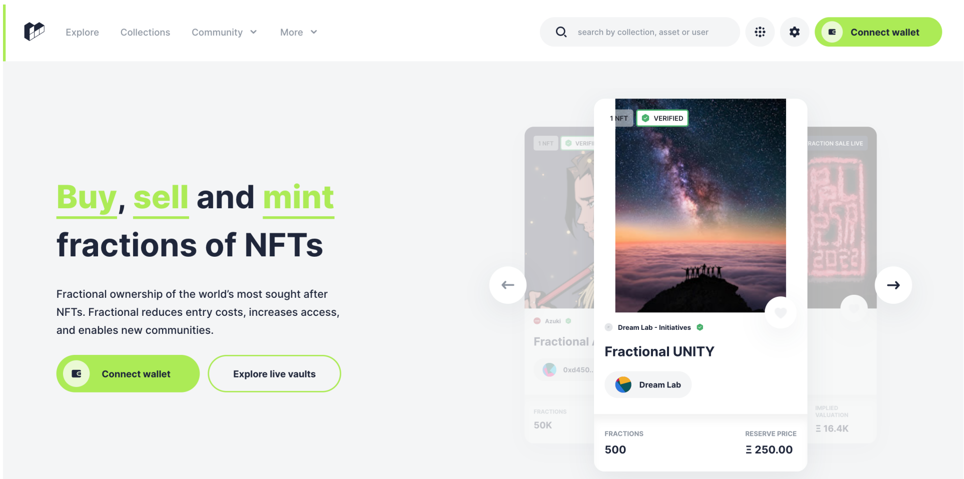
From that point, users could freely mint NFTs on the platform and the only requirement was to own enough crypto assets in a connected wallet for being able to pay the network fee [62]. This led to an exponential increase in counterfeit assets and to an increased reluctance on behalf of both artists and investors to trust OpenSea, despite their claims about the ongoing efforts they take to minimise these practices [62].

Besides this, OpenSea allegedly set the security objectives as one of the lower priorities [62], and this statement is backed by the most recent phishing attack that took place on the platform in February 2022 [63]. Reportedly, a total of 254 NFTs valued at approximately USD 1.7M were stolen from 32 users, as they were lured into signing a partial smart contract with their private key that allowed attackers to transfer ownership of the NFT without paying [62].

Another aspect that needs to be considered is that even if the platform supports several networks, most of the assets are still being minted and traded on Ethereum [57]. As recently Ethereum gas fees have surged [45], OpenSea has been charging creators a first-time minting fee that can rise at up to USD 400. Consequently, this is another reason that keeps crypto artists reluctant, as the low initial exposure of their assets does not guarantee a break-even point.

3.3.2 | Fractional

In the NFT ecosystem, there is one more ownership model that is enabled by the Fractional platform. It is called 'fractional ownership' and it refers to joining an investment pool where several investors purchase a single NFT [53]. The Fractional platform headquartered in New York City offers exclusively this ability to its users, so that artists can partition their artworks into the desired amount of fractions and list it, while investors can purchase the desired amount of fractions of an NFT, based on the listing price [64].



Fractional ownership of the world's most sought after NFTs. Fractional reduces entry costs, increases access, and enables new communities.

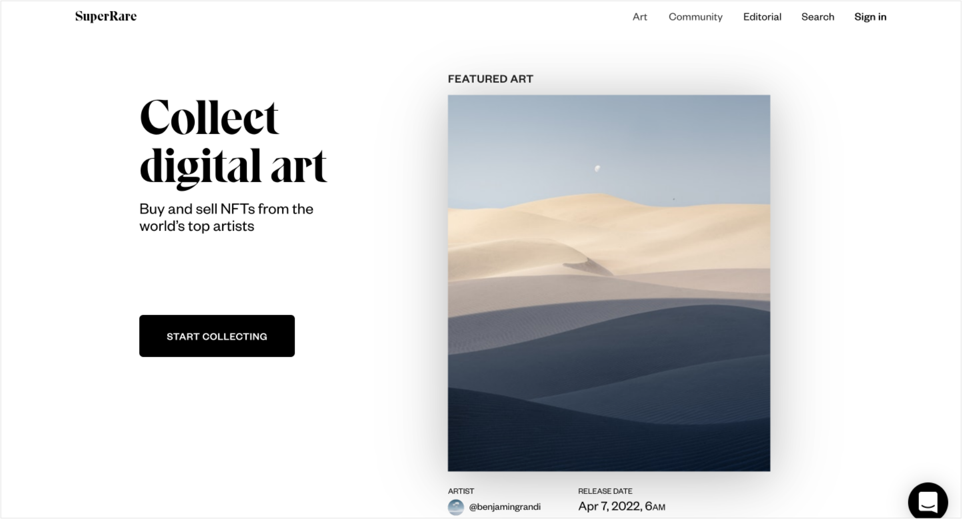
Figure 3.4: Fractional Platform. Source: [64]

This might seem a promising option that can democratise access to a fairly intangible asset class, considering the millions of dollars valuation of some representatives. However, reportedly the locked value in NFT fraction based crypto exchanges started to plummet, which indicates a diminishing interest in this ownership model [64]. Besides that, an even more concerning issue is that fractionalising NFTs could be deemed as a violation of securities laws, as the U.S. Securities and Exchange Commission (SEC) has already started an investigation on this asset class in March 2022 [53, 65].

3.3.3 | SuperRare

Unlike the previously mentioned case studies, SuperRare is an art-focused NFT marketplace that was launched in 2018 [66]. Still featuring a wide variety of digital art, including illustrations, photography, videography and GIFs, the platform also offers artists the possibility to list their assets at a fixed price or an auction [67].

One more area where SuperRare distinguishes itself from other marketplaces is the artists' access to the platform, which is limited to a small number of artists per month [67]. Consequently, the platform representatives go through a selection process so that the overall level of quality for the NFT listings is increased. Besides this, all the NFTs and the collections that are publicly available on the platform are closely curated [62, 66]. This naturally brings a higher degree of trust on behalf of the investors.



Collect digital art

Buy and sell NFTs from the world's top artists

Figure 3.5: SuperRare Platform. Source: [67]

Nevertheless, SuperRare only operates on the Ethereum mainnet and hence, the supporting currency is ETH [66]. This can be perceived as a drawback for several prospective users, in the context of high ETH transaction fees and also, the release of several layer 2 blockchains that support NFT transactions and feature lower transaction costs and energy consumption rates [66].

3.4 | Evaluation of State of the Art

Within the current section, it was possible to obtain an overview on the scientific literature available at the time, the inherent technologies and their intricacies that enable the NFT ecosystem and also, some relevant existing NFT marketplaces with their strengths and weaknesses. Since a summary of the Literature Review was already provided in subsection 3.1.3, the current evaluation only refers to the technical aspects and the selected case studies.

The two main networks that were analysed were Ethereum and Polygon and each of them comes with a set of advantages and drawbacks. At the time of writing, Ethereum is more widely used and there are several resources in the blockchain and crypto developers community. However, Polygon is gaining traction due to providing increased throughput, decreased transaction fees and a reduced environmental impact, based on the used PoS consensus mechanism [48]. For these reasons, using the Polygon network is considered for developing a functional prototype as one of the outcomes of the thesis.

In terms of NFT standards, the most relevant to consider is the ERC-721, as it is aimed specifically at non-fungible tokens and does not introduce any other use cases as semi-fungible tokens [52], which are outside the scope of the current research theme. Furthermore, despite an increased difficulty level, decentralised data storage is also a viable option to consider for the prototype, since this approach preserves the files' metadata once stored, as opposed to centralised file storage such as the case of cloud service providers [53].

Regarding the described case studies, it is possible to state that each of them faces a different set of challenges. OpenSea confronts with a considerable amount of listed counterfeits and plagiarised works and the Fractional platform experiences a decreased interest in their value proposition [53], while it is also suspected of breaching securities law, due to the inherent 'fractional ownership' model that it features [64].

Furthermore, SuperRare only operates in early access mode, being highly restrictive in terms of the number of creators that it accepts on the platform and above all that, it only uses the Ethereum mainnet which comes at the cost of high network fees and slow processing of transactions [66].

In general, it is possible to assess that what each marketplace is missing is a possibility to identify the sellers segment, that includes digital artists, but are not limited to that. This is due to the fact that once an artist has sold an NFT, the asset can further be resold in the same marketplace or even in others, fact that makes it more difficult to assess whether a listed NFT represents original content or not [27]. At the same time, an identification system for the NFT sellers should carefully be balanced with respecting the users' privacy, that was initially one of the main value propositions of blockchain technology [54].

Consequently, it can be derived from the analysed case studies that there is a need for a better identification system for the users, and more precisely for the sellers of NFTs, as this would increase consumers' trust in the authenticity of the listed artworks, and also, in the NFT industry overall. Needless to say, one should always exercise caution when entering the NFT market and acknowledge the level of risk that investing in this asset class entails.

4 Data Analysis and Evaluation

4.1 | Expert Interviews

For the purpose of gaining a better understanding of the technicalities behind NFTs and their current shortcomings, a qualitative data analysis would be elaborated within this section. Consequently, two structured interviews with experts in the field were conducted. They were aimed at exploring what is missing from a technical perspective and what could be done further in order to prevent malicious activity as cyber theft and counterfeits in the NFT industry.

The interviewees were intentionally chosen as coming from different backgrounds, to prevent bias and to enable an extensive comparison of different perspectives and visions. As such, the first respondent was Christian Carle, Social Support Specialist working a publicly traded crypto company from the US. The second respondent preferred to remain anonymous for protecting his identity in the space, and for this reason he will be referred to as *Liam*. However, it is possible to disclose that he is a Senior Software Engineer, highly knowledgeable in Web3, DeFi and blockchain development.

The set of questions followed the pattern of open-ended questions, for the purpose of exploring new ideas and obtaining comprehensive answers. All of the questions were derived from findings mentioned above, in different sections of the thesis.

As such, for obtaining complete transparency in the data collection process and questions' origin, it is possible to state that while the first question was general, for getting to know the respondent better, questions number 2 and 3 were related to the Literature review section (3.1), challenging M. Zeilinger's article [37] and his views about NFTs artificially creating scarcity and U.W. Chohan's paper on the intrinsic value of NFTs [38]. Further, questions from 4 to 7 were derived from the Case Studies subsection (3.3) under the State of the Art and more precisely, to OpenSea's statement about the considerable amount of counterfeit items stored on their platform [17].

Further, questions 8 and 9 specifically refer to the NFT paper by Wang et al [10], that mentions the outdated regulatory frameworks, and also to the first research sub-question, relevant for designing a comprehensive system. Questions 10 and 11 are derived from the same paper, but they relate more to the trade-off between anonymity and possible legal pitfalls of such platforms.

While the current section presents a summary of the extracted key takeaways, the complete interview transcripts can be found in the Appendices section (A.1).

After getting to know the respondents with an introductory question, it was possible to assess, based on their subsequent responses, that Ethereum still has a wide market share in NFT transactions. Furthermore, the novelty factor is brought by the visual attractiveness NFTs bring, as compared to 'traditional' blockchain systems, so this might accelerate general adoption of crypto in general.

When asked about what was missing in the NFT space, both respondents agreed upon the technical difficulties related to entering the market. Audiences are not educated enough and they risk to fall prey to fraud attempts. Subsequently, regarding verifying asset authenticity, Christian suggested to verify projects' social media accounts and the communities around them, besides the smart contracts' addresses in Etherscan for ensuring that circulating supply goes both in and out. According to Liam, verification depends on the type of NFT, but often it reduces to verifying that the smart contract to interact with actually has the expected address.

When being asked about solving the counterfeiting issue, the respondents had diverging opinions. Christian suggested that marketplaces *should have a process to have legitimate projects on their accounts*, while Liam challenged the question, stating that the industry tends to move the other way, meaning that they are not likely to impose such restrictions. This is due to the fact that the most common counterfeiting method is actually providing different smart contract addresses for users to interact with.

For preventing cyber theft, Christian advocated for educating the audience and teaching users on how to avoid becoming victims of scams, phishing or social engineering attacks. Besides that, Liam recommended building stronger wallets that have a registry on-chain, together with users being able to vote for contracts for achieving a social consensus. Also according to him, platform liability should only be a requirement if they make use of a centralised layer on top of the blockchain capabilities, because that denotes a centralised entity being actively involved and possibly interfering with the purpose of a system that is supposed to be decentralised.

Moreover, both Christian and Liam mentioned that a smart contract cannot be counterfeited in itself, because it is inherently unique. The connected media files can be similar or even duplicates, fact that can lure investors into buying a project or NFT asset that is nothing but a reproduction of the original one.

To conclude, industry experts can tend to be evangelists in regards to the trade-off between the degree of decentralisation and the security needs of the general users. While Liam would prefer using a fully decentralised platform, bearing a greater exposure to threats and risk of cyber attacks, Christian admitted that platforms should be liable for the content they host and they should have a better process of curating authentic projects. At the same time, a key takeaway from the interviews is that there is a clear distinction in an NFT smart contract address that cannot be counterfeit and a connected media file, that could be downloaded and resold within another NFT smart contract. This is why users need to ensure that the addresses they interact with are the correct ones, before paying attention to the visuals that they embed.

Further, a closing thought expressed by Christian indicated that a highly valuable asset of the NFT industry for him was the community and the feeling of belonging. This makes fraud prevention mechanisms even more desired in the ecosystem, as they would contribute to strengthening the community and enhancing a more widespread adoption rate.

4.2 | User Survey

This research survey is aimed at collecting information on the adoption rate of this new technology and on potential concerns that hold people back from entering the NFT industry. As such, it was possible to retrieve a considerable sample size of the potential users' perspectives, needs and expectations towards the NFT ecosystem and possibly an NFT marketplace.

Therefore, the user survey was distributed to several crypto-related LinkedIn groups and work-related Slack channels, with most of the respondents being located in the United States. The aim was to target respondents who already had an insight in the cryptocurrency world. More precisely, people who had at least heard about blockchain, or who have some interest in blockchain or even in NFTs. By following this approach, it was possible to obtain more valuable insight from direct prospective users of such a platform, as opposed to querying arbitrary respondents who could possibly have no knowledge in the area.

A total number of 82 effective responses were collected in a time span of a week, as it can also be seen in the Appendices section (A.2). Accordingly, the results would be analysed in this section.

Furthermore, the survey questions have also been derived from different sections and findings above. In a brief, questions 1 to 4 were opening questions, with the purpose of getting to understand the respondents demographics, education levels and knowledge in the blockchain area. Questions 5 and 6 included options and criteria based on the conflicting attitudes observed towards NFTs in the Literature review (3.1) [37, 36]. Questions 7 and 8 focus on concerns derived from the Case Studies (3.3), with counterfeit assets stored on OpenSea and concerns over securities law violation by Fractional raised by the SEC [17, 65]. Also questions 9 to 11 relate to the State of the Art conclusion and what features could be derived for building a more trustworthy platform.

The survey started with a question related to the respondents' age group. 81.7% of them were millennials or younger (born after 1980), while only 18.3% were born before 1981. Regarding the educational background, the data showed that 82.9% of respondents were university graduates or even had a higher degree (Master's degree or PhD).

Moreover, it is worth mentioning that the next three questions were intended to discover how the respondents positioned themselves when considering cryptocurrency and blockchain technologies. Overall, on a scale from 1 to 5, most of the respondents (86.6%) claimed to be knowledgeable about cryptocurrencies and/or blockchain technology, with 13.4% of them being highly knowledgeable.

Furthermore, a more specific question highlights that over a half of the respondents (52.4%) were interested in both crypto and NFTs or even already had contact with the crypto world/NFTs.

As the next question represents one of the key aspects of the current research survey, displaying the main reasons that would lead respondents to use NFTs, the question was in the shape of a multiple choice, with an open-ended 'Other' option, intentionally left for capturing more insights and for letting them space without limited options. More than a half (57.3%) of the respondents claimed that financial gains are the main reason that could lead them to use NFTs, closely followed by their interest in the technology (47.6%). Also some of the respondents have chosen to write their own specific reasons such as utility or community.

One of the central questions raised an important aspect related to the concerns that people might have in regards to the current state of NFT technology and the existing marketplaces. 56% of the respondents were concerned about missing regulation and unknown risks. Also, 34.1% indicated that large amount of counterfeits are worrying them the most. Besides this, the novelty of the technology scored 28%, followed by the same percentage for the 'unknown risks'. The open-ended side of this particular question revealed worries about the current state of the market (a potential price bubble), security aspects, expenses, environmental concerns and money laundering activities.

A key takeaway from the following question is that more than a half of the participants stated that any of the previously mentioned concerns would block them from entering the NFT market (61%). Nevertheless, 26.8% denied these barriers and would still participate. It is relevant to state that this specific question highlighted users' primary need for a more secure NFT environment, before they can trust it and onboard the market.

On a roadblock to NFT adoption, 51.2% of the respondents manifested their lack of interest in using a platform for trading NFT art, given the current state of the market and the aforementioned concerns that they had. Notably, when asked if they could trust such a system, 33% of the respondents indicated their lack of trust.

In addition, the last but one question was aimed to investigate what makes an NFT marketplace trustworthy from the respondents' perspective. Verified accounts was the most voted option (58.5%), followed by the inability to change files metadata (34.1%). Apart from the already provided options, some of respondents also suggested notable aspects in regards to the adoption of better regulation and vetting legitimate projects.

Within the last open question, participants provided their feedback and gave some relevant suggestions. One of the most thoughtful comments reflected that 'a big barrier to NFTs is digital literacy (knowledge of the cyber space and access to easily acquired knowledge about blockchain and NFTs...)', while another one also mentioned the need for educating the audiences before they can enter the market as buyers or sellers.

Still, the final open-ended question raised some controversy, based on the strong opinions and heated arguments that some respondents had, either pro or against NFTs. This is a confirmation that the surveyed population was truly committed to share their actual thoughts and concerns, and that both those in favour or against the NFT industry brought their genuine perspectives that will contribute to the current research in the uttermost manner.

To sum up, this study spotlights that even if the novelty of blockchain technology and the NFT concept raised skepticism and concerns related to the security aspects and the trustworthiness of currently available marketplaces, there is still a confirmed willingness of users to participate in a well regulated, more secure and transparent NFT ecosystem.

Therefore, all the meaningful information retrieved from the the user survey contributes to key takeaways that would be further used as solid pillars within the next phase of the thesis, especially for considering use cases and functional requirements for the prototype to be developed.

5 System Requirements Engineering

5.1 | Ideation Process

For the purpose of requirements engineering, a vital constituent from the prism of achieving the goals of the current Master's thesis and project, this section builds on top of the already accumulated information from the previous data analysis and evaluation section.

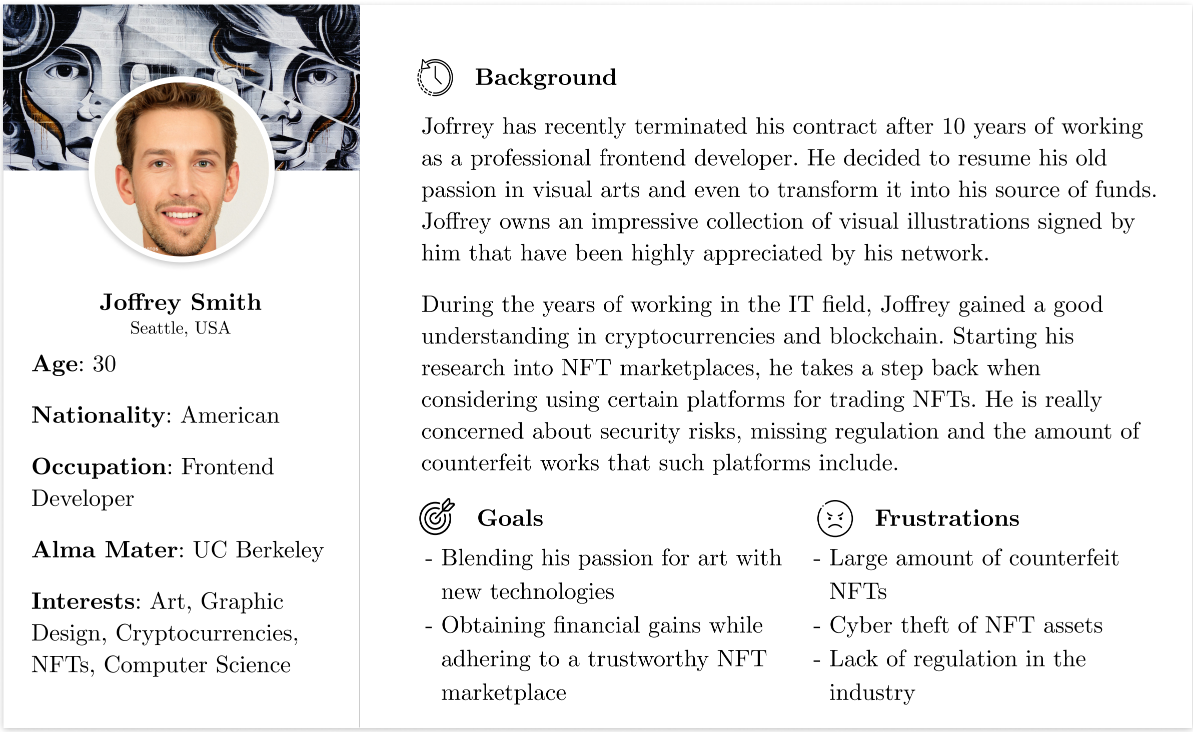
Further, it maps to the 'Ideate' stage from the Design Thinking Process and it comprises the steps of identifying personas, shaping user scenario based on them and also, sketching the use case diagrams derived from the former steps.

5.1.1 | Identifying Personas

The definition of a 'persona' stands in a fictional character or a partial identity created to represent the main user types that would interact with the proposed system in a specific situation or context [68].

This is a step required to distinguish and determine the effective target audience that the current solution is addressing, in order to identify and observe the actual potential users types and their behaviour, patterns, needs and expectations [68]. This would later serve as a solid pillar to consolidate the next phase of the implementation phase.

In addition to that, the persona reflects especially upon data collected from the user survey presented in section 4.2, that has a considerable sample size of 82 respondents. That would be further used for shaping the user scenarios. Hence, the user persona would be described below.



Joffrey Smith
Seattle, USA

Age: 30

Nationality: American

Occupation: Frontend Developer

Alma Mater: UC Berkeley

Interests: Art, Graphic Design, Cryptocurrencies, NFTs, Computer Science

Background

Jofrrey has recently terminated his contract after 10 years of working as a professional frontend developer. He decided to resume his old passion in visual arts and even to transform it into his source of funds. Joffrey owns an impressive collection of visual illustrations signed by him that have been highly appreciated by his network.

During the years of working in the IT field, Joffrey gained a good understanding in cryptocurrencies and blockchain. Starting his research into NFT marketplaces, he takes a step back when considering using certain platforms for trading NFTs. He is really concerned about security risks, missing regulation and the amount of counterfeit works that such platforms include.

Goals

- Blending his passion for art with new technologies
- Obtaining financial gains while adhering to a trustworthy NFT marketplace

Frustrations

- Large amount of counterfeit NFTs
- Cyber theft of NFT assets
- Lack of regulation in the industry

Figure 5.1: Persona | Joffrey Smith

5.1.2 | Scenario

The following scenario describes the interaction between a user and the system to be developed. The user interacting with the system was deliberately chosen as being both a creator and an investor/collector, for demonstrating the ability to allow more than a single role appended to each user.

Joffrey is an ambitious man that decided to invest all of his time in his passion. He used to work as a front end developer in New York City, but after 10 years of hard working in the IT field, he chooses to follow one of his first passions - graphic arts.

Since high-school, Joffrey had an interest into visuals and graphic arts but his parents had never encouraged him to follow this path. Hence, he graduated a Computer Science program. However, he never gave up on his first passion and therefore he practiced his artistic skills at a hobby level. He owns an impressive collection of visual illustrations that was never exposed before.

Still, all the years spent in the IT sector incentivised him in learning new technologies and trends such as blockchain and cryptocurrencies. With a strong analytical mindset and a good understanding in the crypto world, he decides to blend these new technologies with his passion.

He starts by researching the best options for digitally selling some of his visual illustrations. However, Joffrey has many concerns when trying to adhere to a trading platform. He is worried by the fact that several platforms lack well established regulatory *framework, as well as important security measures to prevent associated risks.*

However, Joffrey did not give up to his plan, so he found the `Smart NFT` *platform that caught his attention. After opening it, Joffrey is able to navigate through the platform in a transparent manner. He can browse through different NFT classes, view their transactions history, or find and view other user profiles.*

Even if at the first glance, he is still skeptical when it comes to security risks, Joffrey decided to create his own account and to join the platform. Then, he tries to mint his very first visual illustration NFT in order to sell it. Suddenly, a pop-up message requests him to submit a KYC form before being able to perform such actions.

Joffrey is truly impressed by this feature and becomes more enthusiastic and confident that this platform would satisfy his needs in a more secure manner, protecting him and others from cyber theft and fraud. This would help creating a trustworthy digital ecosystem by encouraging both artist as Joffrey to become part of it, but also art consumers to buy digital art and to support them.

After his KYC request gets approved, Joffrey releases his first NFT collection and starts getting traction within the community. Weeks later, Joffrey decides to support the community and to also invest in it by purchasing from time to time digital art from his favourite artists. Since he has already had his KYC request approved, he can as well purchase NFTs on the platform, besides being able to sell, so he is currently both a creator and a collector.

5.1.3 | Use Case Diagrams

In Unified Modeling Language, there is a category of diagrams known as Use Case Diagrams. Accordingly, this type of diagrams are an effective technique providing a simple visual representation used to specify the expected use cases that potential users can trigger while interacting with a system [69].

Consequently, the previous subsection containing the user scenario would be used as a key concept in modeling the use case diagrams. For a comprehensive work, two different use cases would be used in order to specify some of the relationships between actors and the system proposed, drawing attention to how non-authenticated vs authenticated users/actors would interact with the system. Further, the action of authenticating a user is performed by connecting a crypto wallet to the dApp.

It is also worth mentioning that actions such as *minting*, *selling* and *buying* an NFT are all conditioned by the action of *submitting a KYC request form*, as illustrated in figure 5.3. This use case also implies that the request must further be approved by the system administrator, before *minting*, *buying* and *selling* can be performed.

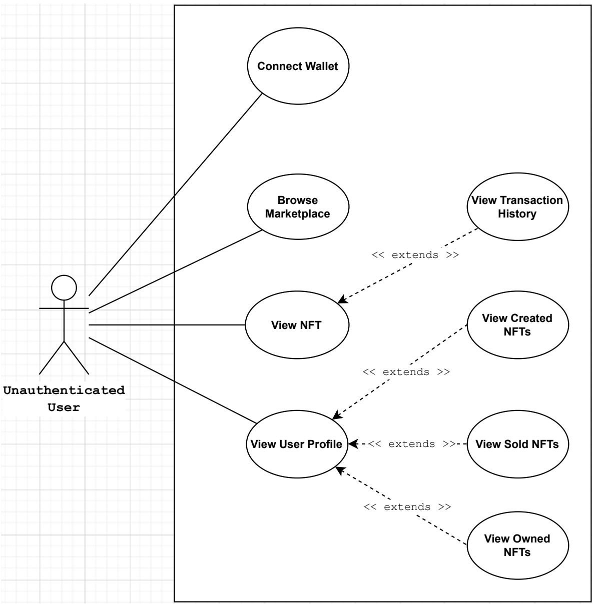


Figure 5.2: Use Case Diagram | Unauthenticated User

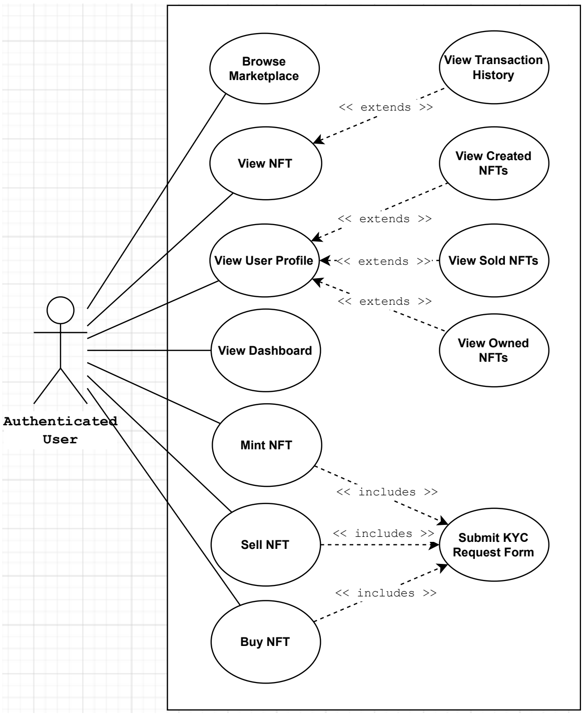


Figure 5.3: Use Case Diagram | Authenticated User

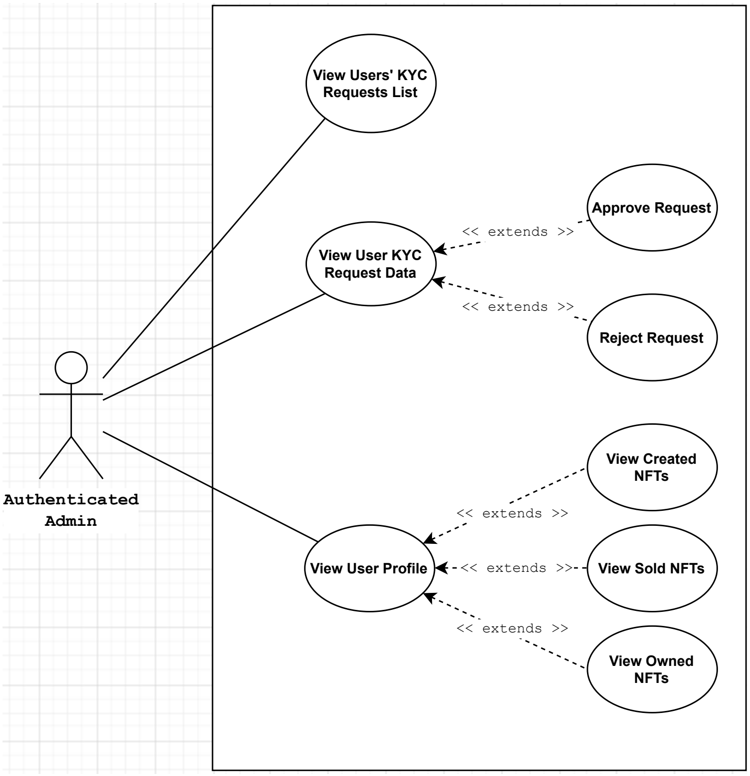


Figure 5.4: Use Case Diagram | Authenticated Admin

5.2 | Requirements Specification

With the accumulated amount of information, the system requirements can be specified by considering the different sections and data retrieved as their outcome. These conclusions serve as a solid foundation for the decisions to be made for building a functional prototype that can demonstrate the capabilities that are needed and that fills the gap existent in the NFT ecosystem. It is necessary to state that the set of requirements only represents the first iteration of the product to be built, due to the agile approach in coordination with the Design thinking process being employed.

The requirements are initially split between functional and non-functional requirements, the former referring to what does the system perform and the latter to how does the system work and under what parameters [69]. Requirements from both categories are prioritised with the MoSCoW method [69] and are linked to the relevant sections of the thesis where they have been derived from. At the same time, non-functional requirements are further categorised with the FURPS+ method (acronym for Functionality, Usability, Reliability, Performance and Supportability), developed at Hewlett Packard [70] and they are also linked to their corresponding functional requirements counterparties.

5.2.1 | Functional Requirements

For complete transparency, it is necessary to clarify the terminology used in the upcoming set of requirements. Therefore, the term 'authenticated users' is used as an umbrella term that includes all users who have connected their crypto wallet to the dApp. At the same time, the 'approved users' are those whose KYC application forms have been verified and approved by the system administrators and who are authenticated in their accounts by the time they perform a transaction.

ID	Functional Requirement	MoSCoW	Source
1	The system must consist in a decentralised front-end application connecting to a smart contract interface.	MUST	3
2	The user must be able to connect their crypto wallet browser extension to the system.	MUST	3
3	The system must allow all users to browse through an NFT marketplace.	MUST	3.4
4	The system must allow all users access to a Learning centre including links to reputable resources for educating the audience and to crypto-related news articles.	MUST	4.1, 4.2
5	The system must allow all users to view all metadata related to NFT listings.	MUST	3.4, 4.1
6	The system must allow all users to view the partial profiles of verified users that include the set of NFTs that they created, sold and owned.	MUST	5.1.3
7	The system must allow users who have connected their crypto wallets to submit a KYC verification request form.	MUST	4.2, 5.1.3
8	The system must encrypt sensitive user data sent within the KYC request form.	MUST	5.1.3
9	The system must allow authenticated *admin* user types to decrypt sensitive user data for verification purposes.	MUST	5.1.3
10	The authenticated *admin* user type must be able to approve or reject a user's KYC request form.	MUST	5.1.3
11	The approved user must be able to mint an NFT.	MUST	3.1, 3.4
12	The approved user must be able to buy an NFT.	MUST	3.3, 4.1
13	The approved user must be able to sell an NFT.	MUST	3.3, 4.1
14	The approved user should be able to access a personalised dashboard containing the historical values of their NFT portfolio and trading KPIs.	SHOULD	4.2
15	The system could require content curation before NFT assets are listed on the public marketplace.	COULD	4.2

Table 5.1: Functional Requirements

5.2.2 | Non-Functional Requirements

As expected, a majority of the non-functional requirements have been derived from the Technological enablers section (3.2), as they relate to the inner workings of the system to be built. However, several aspects have been accounted for, such as the feedback obtained from the expert interviews or learning retrieved from the State of the Art section (3).

ID	Non-Functional Requirement	MoSCoW	FURPS+	FR	Source
1	The system must use the Polygon blockchain network with Solidity smart contracts as the underlying decentralised layer.	MUST	Design	1	3.2, 4.1
2	The system must embed a NextJS front-end application that is able to call smart contract functions via a third party NodeJS library.	MUST	Implementation, Interface	1	3.2
3	The system must support connections to the Metamask browser wallet extension.	MUST	Interface	2	3.2, 4.1
4	The system must store NFT assets on the Polygon network and the corresponding file metadata using the decentralised IPFS protocol, for preserving data integrity.	MUST	Reliability, Implementation	3, 5, 11	3.1.3, 3.2
5	The system must display the ownership structure and origin of each listed NFT asset, as the wallet addresses of the creators and owners, linked to the corresponding user profiles.	MUST	Functionality, Usability	5, 6	3.4, 4.2
6	The system must include a KYC verification request form that must be accessible by users with connected crypto wallets, but who did not previously submit the form.	MUST	Usability	7	4.2, 5.1.3
7	The KYC verification form must adhere to and follow the general standards and questions that are usually addressed in banking institutions' KYC processes.	MUST	Functionality	7	4.2
8	The system must use the AES symmetric encryption algorithm to encrypt sensitive user data sent with the KYC request form before storing it on-chain, in an immutable format.	MUST	Reliability, Implementation	7, 8, 9	3.2, 5.1.3
9	The system must store files added as documentation during the KYC process using the IPFS protocol, for preventing tampering with their metadata.	MUST	Reliability, Implementation	7, 8	3.2
10	The system must generate user profiles for the users who have successfully submitted the KYC verification request form.	MUST	Functionality, Usability	6	4.2
11	The KYC smart contract must provide a getter function for fetching the list of users who have submitted a KYC request, that is only callable by admin user types.	MUST	Design	7, 9	5.1.3
12	The system must provide the admin user types with the secret key for decrypting the submitted sensitive user data, for verification purposes.	MUST	Implementation	9	3.2
13	The KYC smart contract must employ functions for approving or rejecting a KYC request that are only callable by admin user types.	MUST	Design	10	5.1.3
14	The system must feature an ERC-721 compliant smart contract for minting non-fungible tokens on the Polygon network, that is only accessible by approved users.	MUST	Implementation	11	3.2
15	The system must employ a marketplace smart contract that provides functions for buying and selling NFT assets, that are only callable by approved users.	MUST	Implementation	12, 13, 14	3.2, 4.2
16	The system must support ETH on the Polygon network as the cryptocurrency of choice for increased performance and reduced network fees.	MUST	Performance, Interface	11, 12, 13	3.2, 3.4
17	The front-end application must re-use components from a GUI components library, for enabling an understandable and easy to use flow for the end users.	MUST	Usability	1, 2	4.1, 4.2
18	The front-end application should compute the sales volume and purchases related to a user for displaying a visual overview of the users' transactions and history.	SHOULD	Functionality, Usability	14	4.2
19	The system won't employ computer vision ML algorithms to verifying the user submissions, and curating them before approving them and publishing them on the platform.	WON'T	Implementation	15	4.1

Table 5.2: Non-Functional Requirements

6 Technical Implementation and Evaluation

It's about taking an idea in your head, and transforming that idea into something real. And that's always going to be a long and difficult process.

Milton Glaser, American graphic designer

6.1 | Concept

Based on the previously defined set of system requirements, it was possible to proceed into the 'Prototype' stage of the Design thinking process and to begin the process of building the functional prototype to demonstrate the aforementioned capabilities.

Consequently, the developed system is named `Smart NFT`, a compound word formed by 'smart' and 'art', as both these terms specify exactly what the platform encompasses. It is an innovative NFT marketplace that not only allows trading of digital assets and collectibles between users, but that is built on cutting-edge technologies that focus on performance, reliability and security.

Besides being built on top of the Polygon blockchain network, one of the platform's main value propositions is the mandatory KYC verification process that stores encrypted data on-chain that all users who perform minting, buying and selling of NFT assets are required to undergo.

KYC is a standard in the financial ecosystem for verifying the identity and business risks associated with a person [71]. Inspired from the traditional banking and investments areas, the KYC process that was introduced enables the user to submit a form containing identification and trading data, so that fraud attempts can be prevented. The most relevant field sets of the KYC form include contact details (email, home address, country of residence), personal details (full name, gender, date of birth, social security number, country of origin) and trading details (expected yearly trading volume, source of funds, Politically Exposed Person - PEP state, sanctions list). All of the declared statements need to be backed by documentation, in terms of passport or ID photo, proof of source of funds document (eg. inheritance, salary slip) or proof of address (most likely a recent utility bill).

Since the submitted form mostly includes sensitive user data, it was necessary to encrypt it with a resilient algorithm (AES-256), so that only authorised users such as the platform administrators or compliance officers would be able to access it. Additionally, for ensuring a persistent and reliable storage and for keeping the platform fully decentralised, the submitted data is being stored on-chain after being encrypted, and the attached documentation is stored using the decentralised IPFS protocol.

As seen in the requirements list, the decision of providing 'on-chain' KYC was based on prospective users' feedback and the data collected from the expert interviews. According to the research data, this mandatory feature would make the platform and the stored user generated content (i.e. NFTs) more trustworthy in the eyes of prospective users and hence, would bring an improvement to the entire NFT ecosystem.

Apart from this, interview and survey respondents expressed the need for educating the audiences before they can comfortably delve into trading NFTs with the peace of mind that they are doing it correctly. Since with the current market state it is not possible to pretend that fraud is not happening in the ecosystem, at a large scale, the platform also features a 'Learning Center' page. Here is where users are directed to external trusted resources and industry news articles, for learning about the basics of blockchain, cryptocurrencies and NFTs. With a thorough documentation of the processes and a clear beginner-friendly explanation of the intricacies of trading NFTs, prospective users are less vulnerable to targeted attacks of any kind (eg. phishing, social engineering).

Considering the aforementioned information, the current section describes the building blocks of the MVP prototype, considering the system architecture, used frameworks and developed features, from a hands-on engineering and coding perspective.

6.2 | System Architecture

After specifying the sets of functional and non-functional requirements, it was possible to define a suitable system architecture that would allow for building a comprehensive system that adheres to the requirements. In general, a blockchain follows an ordinary peer-to-peer architecture, distributed and decentralised, with a set of predefined rules for validating transactions and propagating them to the rest of the nodes.

However, the blockchain in itself is just a constituent part of a holistic system to be built, so an optimal way to describe its architecture is to extrapolate the Model-View-Controller (MVC) pattern towards the use case of the NFT marketplace dApp. The MVC pattern has first been described in 1988 in The Journal of Object Technology as a 'general programming paradigm and methodology' [72] that aims for a clear separation of concerns between the logic of the system (Controller), the data that is being manipulated (Model) and the representation of that data (View) [72]. Further, the application is fully decentralised, as the front-end side of the system is directly connected to the smart contract functionality.

6.2.1 | System Architecture Diagrams

The following subsection describes the system architecture diagrams and their inherent components, as deduced from the set of system requirements. Diagram 6.1 illustrates an MVC based approach towards the building blocks of the system, that are each briefly described below.

Solidity Smart Contracts: Representing the Controller, smart contracts are the backbone of the system, where the entire logic of the application is stored. They are written in Solidity and they are deployed to their own addresses in the Polygon blockchain. In the current shape of the system, there are three different smart contracts in use: an ERC-721 compliant contract for minting NFTs, one for KYC related purposes (adding KYC verification requests, approving or rejecting requests) and one for marketplace transactions (buying or selling NFT assets, viewing owned assets, etc.).

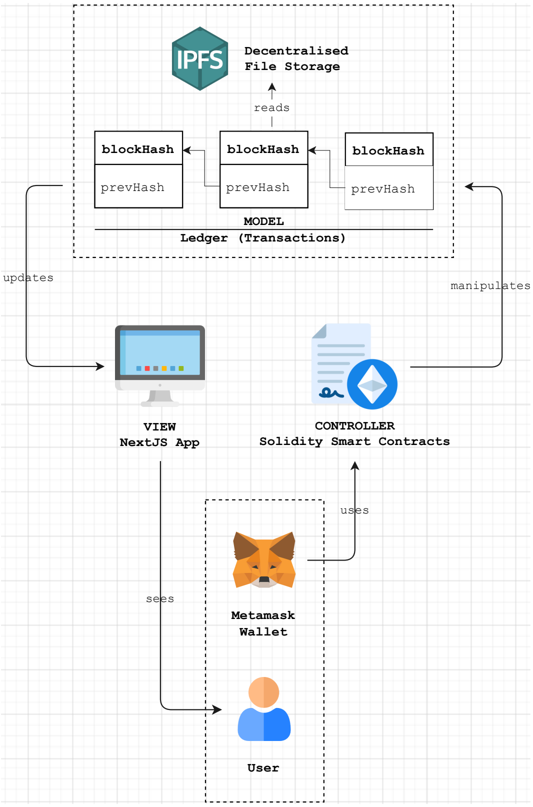


Figure 6.1: Smart NFT | System Architecture Diagram

DLT and IPFS storage: The Model consists in the data being manipulated by the smart contracts and the systems that hold them. The main component that handles the data is the ledger itself, as the distributed and decentralised 'database'-like structure holding transactions' data in an immutable and irreversible fashion. Further, IPFS is the decentralised file storage system used to immutably store the NFTs' associated files, as well as the KYC related user documentation. IPFS has been chosen as a way to increase the availability of the data, since it deters the bottlenecks of a centralised server as a single point of failure.

NextJS Web Application: Even if NextJS is a web development framework that can handle both client and server side code [73], it was only used to create the front-end of the dApp that acts as the View component within the MVC framework. It is the component that visually renders the transaction data representing the Model and it also represents the layer of interaction which is the closest to the user.

Additionally, it is worth mentioning that the user is the entity that interacts with the system, but only via a cryptocurrency wallet; in this case, the MetaMask wallet browser extension. This is because every transaction must be signed by the issuer, either it being of submitting a KYC verification request or minting a new NFT.

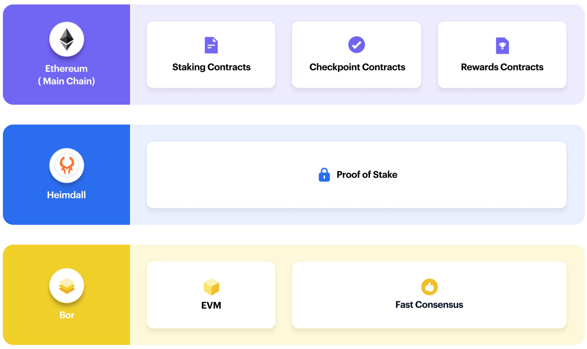
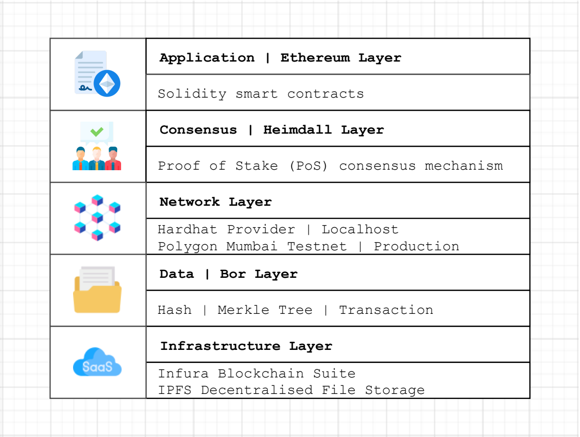


Figure 6.2: Polygon Architecture Diagram. Source: [48]



Application | Ethereum Layer
Solidity smart contracts
Consensus | Heimdall Layer
Proof of Stake (PoS) consensus mechanism
Network Layer
Hardhat Provider | Localhost Polygon Mumbai Testnet | Production
Data | Bor Layer
Hash | Merkle Tree | Transaction
Infrastructure Layer
Infura Blockchain Suite IPFS Decentralised File Storage

Figure 6.3: Smart NFT | Polygon DLT Architecture Diagram

The second set of diagrams illustrated in figures 6.2 and 6.3 refer to the decentralised side of the system. While diagram 6.2 was retrieved from the Polygon documentation [48], the latter was developed from scratch and it represents an extension to the former, for the reason of illustrating the entire decentralised ecosystem in place.

As mentioned in subsection 3.2.1, Polygon is a Layer 2 network, which means that the first layer that it uses is the Ethereum mainnet, where the smart contracts are staked [48]. The second is represented by the Heimdall Layer and it is responsible for enabling the PoS consensus mechanism, while the Bor Layer aggregates transactions into blocks, so it handles the data layer [48].

Accordingly, the extended version was inspired by the OSI model diagram and it includes five layers. The first one is the Application Layer, corresponding to the Ethereum layer from diagram 6.2 and the Solidity smart contracts that are stored on it.

The second is represented by the Consensus Layer and it maps to the Heimdall layer described by the Polygon documentation. Furthermore, the Network layer represents the actual network where the smart contracts are being deployed. As such, there are two different environments in use; a Hardhat Provider has been used in localhost for development purposes, as it locally runs an instance of a blockchain network. In the production environment, smart contracts have been deployed to the Polygon Mumbai TestNet, as the dApp is still a proof of concept and not yet audited for confidently being used on a MainNet.

The Data Layer represents the shape of how data is stored in the Polygon blockchain and it is directly mapped to the Bor Layer. As described by the Polygon documentation, transactions are grouped in blocks and blocks are further stored in the shape of Merkle trees [48]. Nevertheless, the Infrastructure Layer is given by the actual provider that gives access to its blockchain resources, in a similar way to what cloud computing providers do for centralised services. In this case, the Infura Blockchain Suite has been chosen, due to the ability to use a Polygon network and a straightforward integration with an IPFS node for storing files in a decentralised manner [74].

6.3 | Used Frameworks and Libraries

The current subsection briefly illustrates the most relevant frameworks, programming languages and libraries that were used in the development of the `Smart NFT` system. A concise description of the usage is being attributed to each of the enumerated entities.

- `Polygon`: Ethereum-based Layer 2 blockchain platform built for scalability and efficiency [48]. It is used in the `Smart NFT` system as the network provider for avoiding the high fees and efficiency bottlenecks of Ethereum. For this reason, the smart contracts are deployed to the Polygon Mumbai Testnet for being used in the production environment.

- `Hardhat`: An Ethereum development environment that allows for running Solidity smart contracts locally [75]. As Polygon is a Layer 2 solution on top of Ethereum, it is fully compatible with Hardhat.

- `Infura`: Blockchain development suite that provides APIs and developer tools for accessing Ethereum, Polygon and IPFS networks [74]. It is used in the current system for deploying the smart contracts to the Polygon Mumbai Testnet and for connecting to an IPFS network node, for storing files in a decentralised manner.

- `IPFS`: Specifically used within the dApp with the `ipfs-http-client` library, IPFS is a peer-to-peer protocol used for storing data in a distributed file system [55]. It is used within the `Smart NFT` system for storing NFT files metadata and users' documentation submitted with the KYC verification form.

- `MetaMask`: Crypto wallet browser extension that can interact with Ethereum and other Layer 2 blockchains [76]. Used in the system to connect the users, sign and approve transactions.

- `crypto-js`: Library used for encrypting and decrypting sensitive user data stored on-chain within the KYC verification form submission. The encryption algorithm of choice is AES-256, corresponding to a 256 bits key length for increased resilience towards threats.

- `Solidity`: Object-Oriented Programming (OOP) language for implementing smart contracts [41].

- `Chai`: Test Driven Development (TDD) assertion library for NodeJS [77]. It is primarily used in the current project for unit testing the smart contract functions.

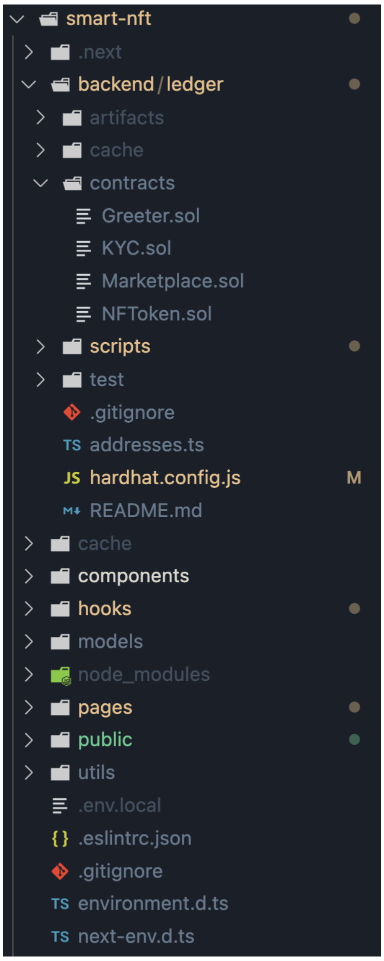
- `Ethers`: Javascript library for interacting with the Ethereum blockchain [78]. Used in `Smart NFT` as a middleware for calling smart contract functions from within the front-end application.

- `NextJS`: Web development framework built on top of React focusing on performance, scalability and server-side rendering (SSR) [73].
- `TypeScript`: A superset of the Javascript programming language that features static type checking capabilities [79]. It is slowly becoming the industry standard and it was used in more than 87% of the codebase, for preventing runtime errors in the dApp and ensuring a high quality codebase.
- `Chakra UI`: A front-end component library for React applications that includes highly customisable reusable components [80]. By using the library, it was possible to achieve a usable and comprehensive front-end solution in a reasonable time frame.

6.4 | Feature Development

The upcoming section focuses on unfolding the intricacies of the codebase, based on the functionalities of the Web3 NFT marketplace. It is worth mentioning that the described functionalities are filtered from the entire list as being some of the most relevant use cases for the purpose of the project. Consequently, the list of features and functionalities is not exhaustive.

6.4.1 | Directory Structure



```
smart-nft
  .next
  backend/ledger
    artifacts
    cache
    contracts
      Greeter.sol
      KYC.sol
      Marketplace.sol
      NFToken.sol
    scripts
    test
    .gitignore
    addresses.ts
    hardhat.config.js                M
    README.md
  cache
  components
  hooks
  models
  node_modules
  pages
  public
  utils
  .env.local
  .eslintrc.json
  .gitignore
  environment.d.ts
  next-env.d.ts
```

Figure 6.4: Smart NFT Project | Directory Structure

For a simple dependency management and overall convenience purposes, the system was developed as a monorepo, where the blockchain-related code shares the same root directory with the front-end application. However, by following industry-standard best practices in both structuring the codebase and code writing, there is a clear distinction between the two sides of the system, as the former is located under `backend/ledger`, while the latter is distributed around the main relevant directories that are usually self-created or provided within a standard NextJS application: `components`, `hooks`, `models`, `pages`, `public` and `utils`.

Starting with the decentralised part of the system, the main folder of interest is `contracts`, as it contains the Solidity smart contracts, each for the purpose defined by their naming convention: `KYC.sol`, `Marketplace.sol` and `NFToken.sol` (the last being the smart contract for minting the NFT).

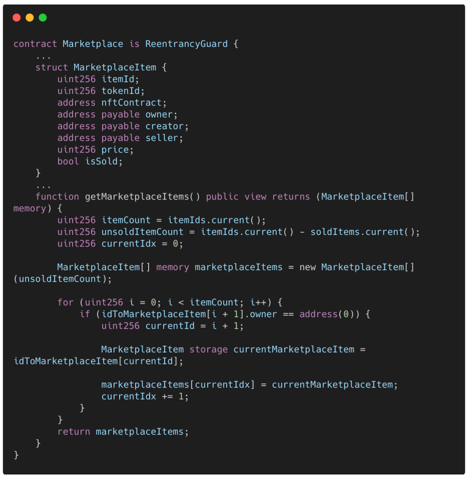
The `artifacts` directory is generated at compile time and it includes the ABI (Application Binary Interface) representations of the smart contracts that will be used for communicating with them. Further, the `scripts` directory contains the deploy script for the smart contracts, while the `test` directory name is self-explanatory.

In the front-end side, the most important directory is `pages`, as the files and directories located under it define the NextJS routes and their corresponding URL paths. The directory also contains `_app.tsx`, which is the entry point of the NextJS application. Each other file under `pages` is a main page that imports several components from the `components` directory, which is also split in several subfolders.

`components/base` includes wrappers for reusable single components imported from the `chakra-ui` library. All the rest are either composite or application-specific components and they are further divided by the purpose they serve (eg. `form`, `kyc-subpages`).

In addition, hooks are special React functions aimed at reusing logic between functional components. For this reason, the custom self-defined hooks have been placed in a dedicated `hooks` directory, so that they can easily be reused across the dApp. Also with the usage of TypeScript, it was necessary to define types and interfaces for the models to manipulate. Consequently, they have all been placed under the `models` directory.

6.4.2 | NFT Marketplace



```
contract Marketplace is ReentrancyGuard {
    ...
    struct MarketplaceItem {
        uint256 itemId;
        uint256 tokenId;
        address nftContract;
        address payable owner;
        address payable creator;
        address payable seller;
        uint256 price;
        bool isSold;
    }
    ...
    function getMarketplaceItems() public view returns (MarketplaceItem[]
memory) {
        uint256 itemCount = itemIds.current();
        uint256 unsoldItemCount = itemIds.current() - soldItems.current();
        uint256 currentIdx = 0;

        MarketplaceItem[] memory marketplaceItems = new MarketplaceItem[]
(unsoldItemCount);

        for (uint256 i = 0; i < itemCount; i++) {
            if (idToMarketplaceItem[i + 1].owner == address(0)) {
                uint256 currentId = i + 1;

                MarketplaceItem storage currentMarketplaceItem =
idToMarketplaceItem[currentId];

                marketplaceItems[currentIdx] = currentMarketplaceItem;
                currentIdx += 1;
            }
        }
        return marketplaceItems;
    }
}
```

Figure 6.5: Marketplace smart contract

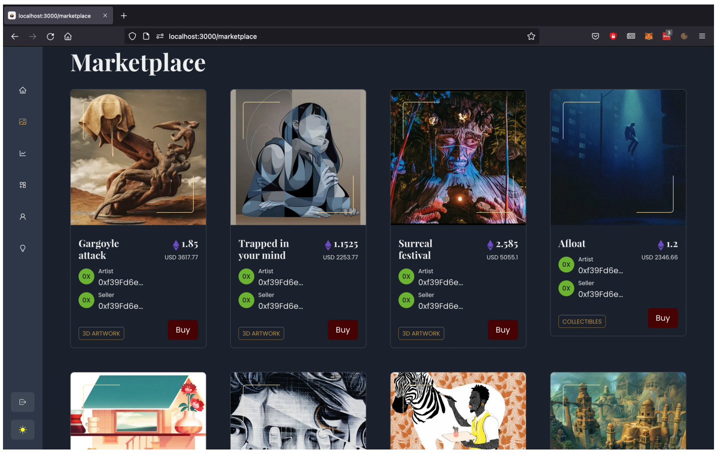
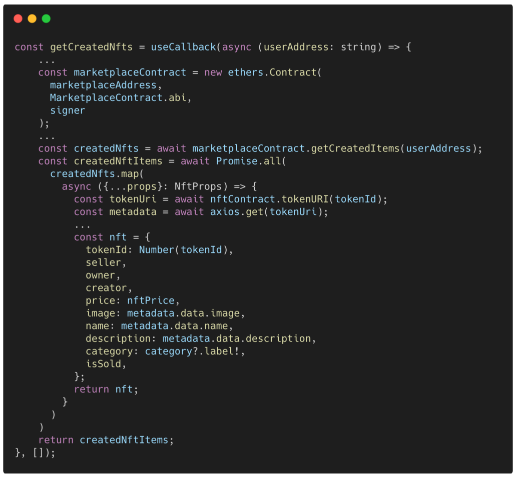


Figure 6.6: Smart NFT | Marketplace Page

The main figure of the `Smart NFT` system is arguably the NFT marketplace page, that renders all the assets that are currently listed for sale. It all starts in the `Marketplace` smart contract, where a `MarketplaceItem` struct (data type) is declared. Then, the `getMarketplaceItems()` function returns an array of `MarketplaceItems` with the items mentioned above and their corresponding struct properties (fig. 6.5).

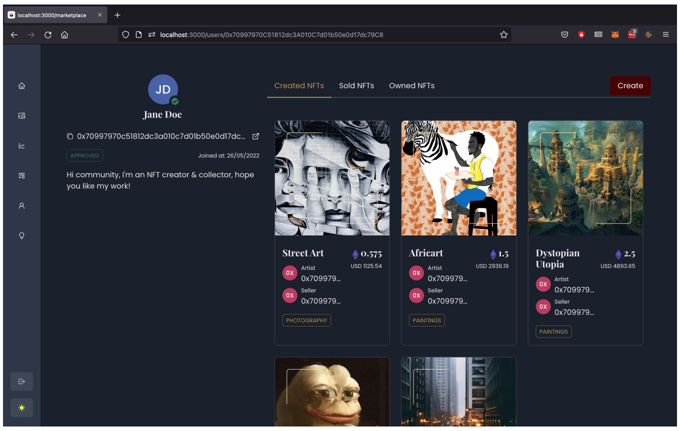
The next step is for the function to be called from the front-end and for this reason, the `useNft()` hook handles all the marketplace and minting related events. To call the function, the hook gets an instance of the `Marketplace` contract by its deployment address and ABI via the Ethers library and asynchronously calls the `getMarketplaceItems()` function from the smart contract. Also, for each NFT item in the array, the `tokenUri` is being used to fetch the corresponding image and metadata from IPFS. The result is then ready to be used in the return statement of the Marketplace page that renders an array of `NftCards`, as seen in figure 6.6.

6.4.3 | User Page



```
const getCreatedNfts = useCallback(async (userAddress: string) => {
    ...
    const marketplaceContract = new ethers.Contract(
      marketplaceAddress,
      MarketplaceContract.abi,
      signer
    );
    ...
    const createdNfts = await marketplaceContract.getCreatedItems(userAddress);
    const createdNftItems = await Promise.all(
      createdNfts.map(
        async ({...props}: NftProps) => {
          const tokenUri = await nftContract.tokenURI(tokenId);
          const metadata = await axios.get(tokenUri);
          ...
          const nft = {
            tokenId: Number(tokenId),
            seller,
            owner,
            creator,
            price: nftPrice,
            image: metadata.data.image,
            name: metadata.data.name,
            description: metadata.data.description,
            category: category?.label!,
            isSold,
          };
          return nft;
        }
      )
    )
    return createdNftItems;
}, []);
```

Figure 6.7: getCreatedNfts() hook function



localhost:3000/marketplace

localhost:3000/users/0x70997970C51812dc3A010C7d01b50e0d17dc79C8

JD

Jane Doe

0x70997970c51812dc3a010c7d01b50e0d17dc...

APPROVED

Joined at: 26/05/2022

Hi community, I'm an NFT creator & collector, hope you like my work!

Figure 6.8: Smart NFT | User Page

As the individual user page returns different arrays of `NftCards` for 'created', 'sold' or 'owned' (purchased) NFTs, it was necessary to add at least two functions in the smart contract (for 'created' and 'owned' NFTs), since the 'owned' category could simply be filtered based on the `isSold` attribute from the 'created' array. As the smart contract functions are highly similar to the one illustrated in figure 6.5, with the difference that they include the user wallet addresses as arguments, figure 6.8 showcases the `getCreatedNfts()` hook function that calls the corresponding smart contract function via the `ethers` API.

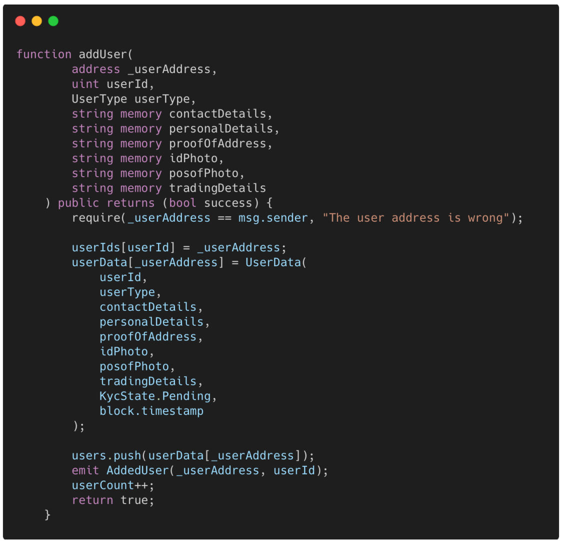
The illustrated hook function and the related one for returning the owned or purchased NFTs are called in the user page, each in a different `Tab` component imported from `Chakra UI`. In this way, the layout of the page remains consistent across each tab and the tab names offer a clear indication to the user of what they contain.

6.4.4 | KYC Verification Process

The KYC verification process consists of a series of conditional events that need to be performed by two actors at minimum. For this, an entire event flow has been modeled, where the first event needs to be triggered by the user requesting to be verified by calling the `addUser()` smart contract function in `KYC.sol`.

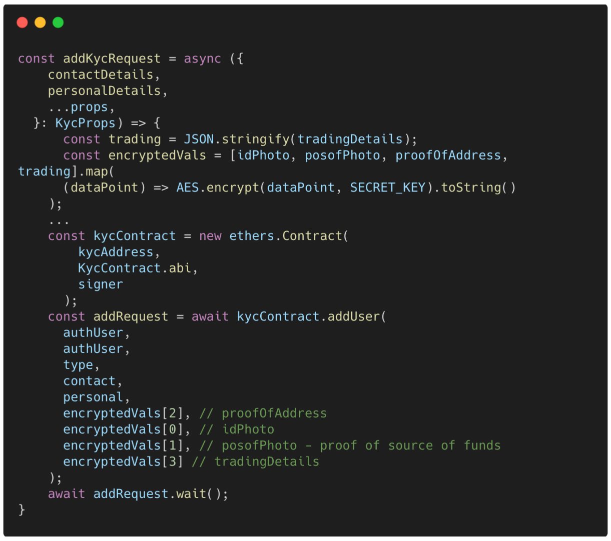
Submitting a KYC verification request

On the smart contract side, a Solidity function shall have a maximum number of arguments and therefore, certain pieces of information submitted by the user have been grouped to form single `string` arguments (eg. `contactDetails`, `tradingDetails`). The arguments list also includes a default `pending` KYC state and a timestamp of the transaction. They are further set to create a new `UserData` struct instance that is further being pushed to the `users` list, while an `AddedUser` event is emitted.



```
function addUser(
        address _userAddress,
        uint userId,
        UserType userType,
        string memory contactDetails,
        string memory personalDetails,
        string memory proofOfAddress,
        string memory idPhoto,
        string memory posofPhoto,
        string memory tradingDetails
    ) public returns (bool success) {
        require(_userAddress == msg.sender, "The user address is wrong");

        userIds[userId] = _userAddress;
        userData[_userAddress] = UserData(
            userId,
            userType,
            contactDetails,
            personalDetails,
            proofOfAddress,
            idPhoto,
            posofPhoto,
            tradingDetails,
            KycState.Pending,
            block.timestamp
        );

        users.push(userData[_userAddress]);
        emit AddedUser(_userAddress, userId);
        userCount++;
        return true;
    }
```

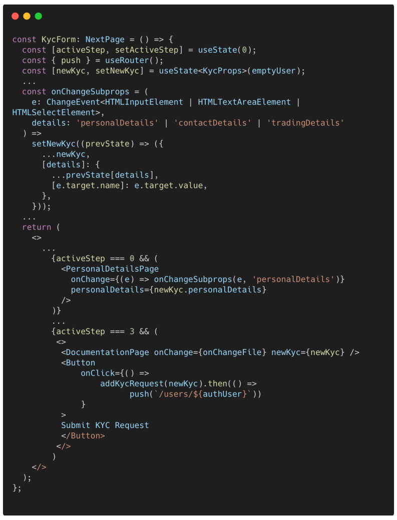
Figure 6.9: addUser() Solidity function



```
const addKycRequest = async ({
    contactDetails,
    personalDetails,
    ...props,
  }: KycProps) => {
      const trading = JSON.stringify(tradingDetails);
      const encryptedVals = [idPhoto, posofPhoto, proofOfAddress,
trading].map(
      (dataPoint) => AES.encrypt(dataPoint, SECRET_KEY).toString()
    );
    ...
    const kycContract = new ethers.Contract(
        kycAddress,
        KycContract.abi,
        signer
      );
    const addRequest = await kycContract.addUser(
      authUser,
      authUser,
      type,
      contact,
      personal,
      encryptedVals[2], // proofOfAddress
      encryptedVals[0], // idPhoto
      encryptedVals[1], // posofPhoto - proof of source of funds
      encryptedVals[3] // tradingDetails
    );
    await addRequest.wait();
}
```

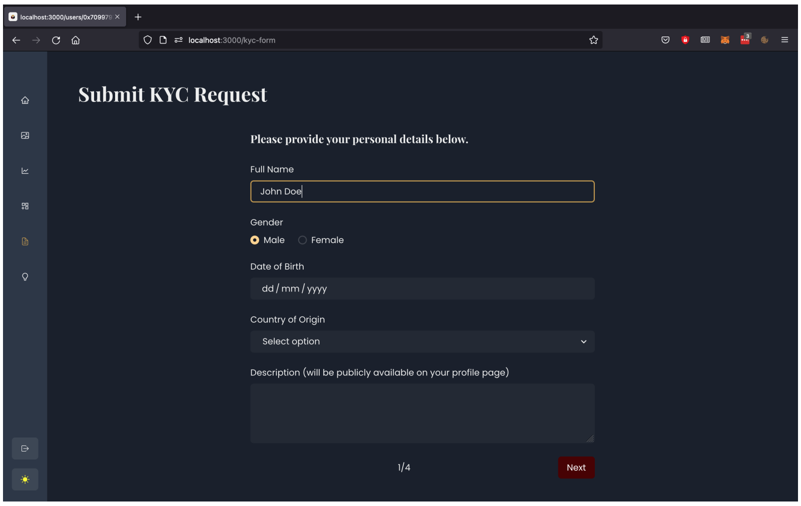
Figure 6.10: addKycRequest() front-end function

In addition, the front-end function calling the smart contract function handles the user generated values before being sent, as they also include sensitive data and Personally Identifiable Information (PII). For this reason, the values of `contactDetails`, `personalDetails` and `tradingDetails` are being being stringified to plain JSON and each output is being encrypted with AES-256 by using a secret key. Only then, values are used as arguments when calling the smart contract function, for being able to protect users identities and sensitive data on-chain.



```
const KycForm: NextPage = () => {
  const [activeStep, setActiveStep] = useState(0);
  const { push } = useRouter();
  const [newKyc, setNewKyc] = useState<KycProps>(emptyUser);
  ...
  const onChangeSubprops = (
    e: ChangeEvent<HTMLInputElement | HTMLTextAreaElement |
HTMLSelectElement>,
    details: 'personalDetails' | 'contactDetails' | 'tradingDetails'
  ) =>
    setNewKyc((prevState) => ({
      ...newKyc,
      [details]: {
        ...prevState[details],
        [e.target.name]: e.target.value,
      },
    }));
  ...
  return (
    <>
      ...
        {activeStep === 0 && (
          <PersonalDetailsPage
            onChange={(e) => onChangeSubprops(e, 'personalDetails')}
            personalDetails={newKyc.personalDetails}
          />
        )}
        ...
        {activeStep === 3 && (
         <>
          <DocumentationPage onChange={onChangeFile} newKyc={newKyc} />
          <Button
              onClick={() =>
                  addKycRequest(newKyc).then(() =>
                        push(`/users/${authUser}`))
              }
          >
          Submit KYC Request
          </Button>
         </>
        )
    </>
  );
};
```

Figure 6.11: KycForm component



Submit KYC Request

Please provide your personal details below.

Full Name
John Doe

Gender
● Male ○ Female

Date of Birth
dd / mm / yyyy

Country of Origin
Select option

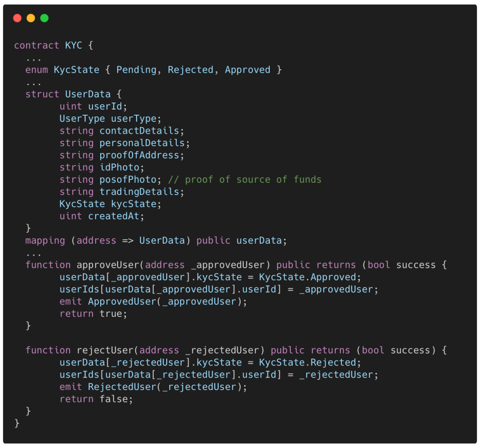
Description (will be publicly available on your profile page)

1/4

Figure 6.12: Smart NFT | KYC Form Page

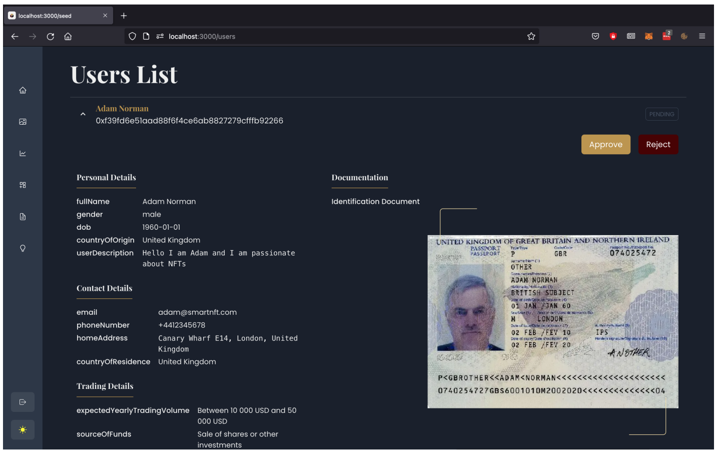
For achieving this on the user facing side, the platform features a multi-page form that splits the input fields according to the category they fit in. Also, the `onChange` event updates the state of each nested key, for obtaining the required number of arguments to be sent to the smart contract function. Moreover, the last form page includes file type input fields for the required documentation. Files metadata is submitted to the IPFS node and the form can only be submitted when all the fields have been completed.

Approving or rejecting a KYC verification request



```
contract KYC {
  ...
  enum KycState { Pending, Rejected, Approved }
  ...
  struct UserData {
        uint userId;
        UserType userType;
        string contactDetails;
        string personalDetails;
        string proofOfAddress;
        string idPhoto;
        string posofPhoto; // proof of source of funds
        string tradingDetails;
        KycState kycState;
        uint createdAt;
  }
  mapping (address => UserData) public userData;
  ...
  function approveUser(address _approvedUser) public returns (bool success {
        userData[_approvedUser].kycState = KycState.Approved;
        userIds[userData[_approvedUser].userId] = _approvedUser;
        emit ApprovedUser(_approvedUser);
        return true;
  }

  function rejectUser(address _rejectedUser) public returns (bool success) {
        userData[_rejectedUser].kycState = KycState.Rejected;
        userIds[userData[_rejectedUser].userId] = _rejectedUser;
        emit RejectedUser(_rejectedUser);
        return false;
  }
}
```

Figure 6.13: Contract functions to verify KYC



Users List

Adam Norman
0xf39fd6e51aad88f6f4ce6ab8827279cfffb92266

Personal Details

fullName Adam Norman
gender male
dob 1960-01-01
countryOfOrigin United Kingdom
userDescription Hello I am Adam and I am passionate about NFTs

Contact Details

email adam@smartnft.com
phoneNumber +4412345678
homeAddress Canary Wharf E14, London, United Kingdom
countryOfResidence United Kingdom

Trading Details

expectedYearlyTradingVolume Between 10 000 USD and 50 000 USD
sourceOfFunds Sale of shares or other investments

Documentation

Identification Document

UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
PASSPORT
PASSEPORT
P
GBR
074025472
OTHER
ADAM NORMAN
BRITISH SUBJECT
01 JAN /JAN 60
M
LONDON
02 FEB /FEV 10
IPS
02 FEB /FEV 20
P<GBROTHER<<ADAM<NORMAN<<<<<<<<<<<<<<<<<<<<<
0740254727GBS6001010M2002020<<<<<<<<<<<<<<04

Figure 6.14: Smart NFT | Approve/Reject user

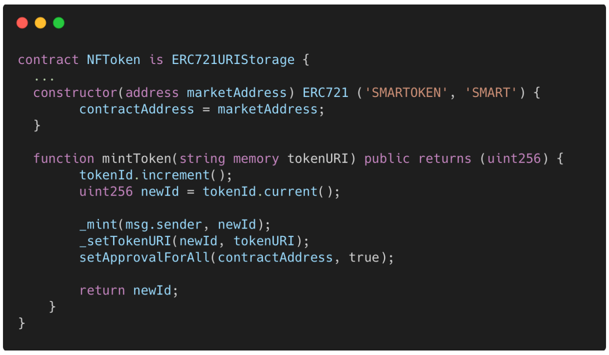
The second part of the verification process is represented by the actual verification step that translates to an approval or rejection event. The verification needs to be performed by an authorised admin user type, who is responsible for checking the documentation that has been submitted by the requesting user.

On the smart contract side, the `approveUser()` and `rejectUser()` functions illustrated in figure 6.13 are first setting the `kycState` attribute of the `userData` object in cause, either to `Rejected` or `Approved`, adding the current `userId` to the the `userIds` mapping and then emitting the corresponding event with the user address argument.

On the front-end, an admin user type needs to be authenticated with Metamask and to have the `admin` attribute appended to their user object. When these conditions are met, the user is authorised to view the `/users` page (fig. 6.14) and to call the `approveUser()` and `rejectUser()` functions, after conducting the due dilligence process and verifying the accuracy of the submitted data points. For this reason, it is possible to assess that the admin user types who could be responsible for this step would most likely be legal and compliance specialists, since the verification process should follow the local laws and regulations that are set to traditional banking institutions.

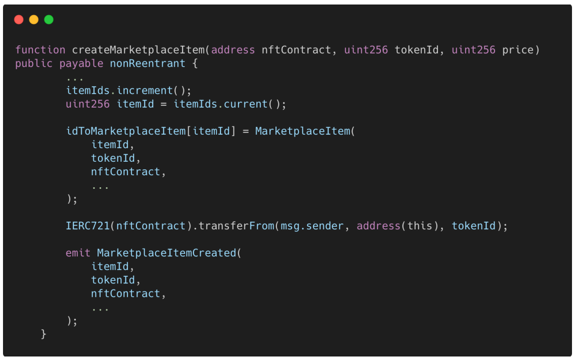
6.4.5 | Minting and Listing an NFT

With an approved KYC request, the user obtains the authorisation to perform transactions on the marketplace. In this regards, both the NFT and the marketplace smart contracts become callable and new NFTs can be minted and listed for sale. As mentioned, there are two different events for this action that are performed by the authorised user: minting and listing an NFT, each corresponding to a function called from a different smart contract.



```
contract NFToken is ERC721URIStorage {
  ...
  constructor(address marketAddress) ERC721 ('SMARTOKEN', 'SMART') {
        contractAddress = marketAddress;
  }

  function mintToken(string memory tokenURI) public returns (uint256) {
        tokenId.increment();
        uint256 newId = tokenId.current();

        _mint(msg.sender, newId);
        _setTokenURI(newId, tokenURI);
        setApprovalForAll(contractAddress, true);

        return newId;
    }
}
```

Figure 6.15: ERC-721 Smart Contract



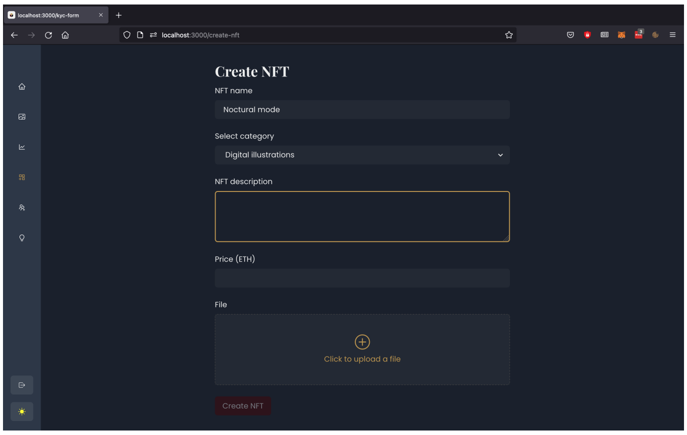
```
function createMarketplaceItem(address nftContract, uint256 tokenId, uint256 price)
public payable nonReentrant {
        ...
        itemIds.increment();
        uint256 itemId = itemIds.current();

        idToMarketplaceItem[itemId] = MarketplaceItem(
            itemId,
            tokenId,
            nftContract,
            ...
        );

        IERC721(nftContract).transferFrom(msg.sender, address(this), tokenId);

        emit MarketplaceItemCreated(
            itemId,
            tokenId,
            nftContract,
            ...
        );
    }
```

Figure 6.16: createMarketplaceItem() Solidity function

The minting function is a straightforward feature offered by the `@openzeppelin/contracts` Solidity library. The smart contract is initiated with an ERC-721 constructor and a generic name of `SMART` is assigned to the non-fungible tokens that it will mint. The minting function first increments the `tokenId` global variable and then calls the `_mint()` function from the library, with the message sender and `tokenId` as arguments. Then, it sets the tokenURI and approves the transaction, followed by returning the new ID of the minted NFT.

The `createMarketplaceItem()` function from the Marketplace contract (fig. 6.16) takes as arguments the NFT contract, tokenId and the price of the item. It appends the arguments as a `MarketplaceItem` struct and then it transfers the tokenId from the message sender to the marketplace contract. Eventually, it emits a `MarketplaceItemCreated` event with the same specified arguments.

On the front-end, the user has to fill in all the fields of a form with values such as asset name, description, category name, price and a file input field, as seen in figure 6.17. When the submit button is pressed, the user is asked to sign and approve each of the two transactions from the connected wallet. Moreover, it is worth mentioning that the only entity that gets stored on-chain is the hashed reference to the NFT item (tokenId), as the file with its metadata are stored in IPFS. After the transactions have successfully been completed, the new entry is being added to the Marketplace screen (fig. 6.6)



Create NFT

NFT name: Noctural mode

Select category: Digital illustrations

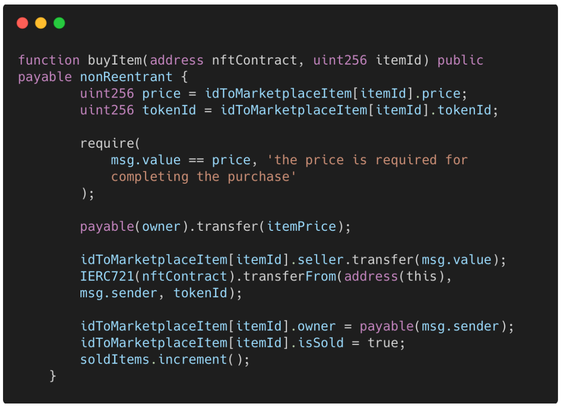
NFT description:

Price (ETH):

File:

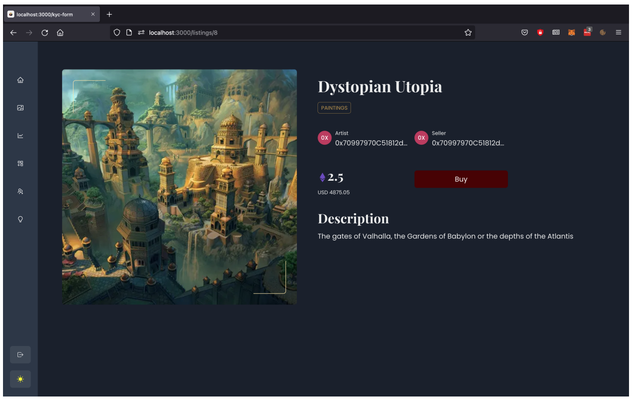
Figure 6.17: Smart NFT | List NFT

6.4.6 | Buying an NFT



```
function buyItem(address nftContract, uint256 itemId) public
payable nonReentrant {
        uint256 price = idToMarketplaceItem[itemId].price;
        uint256 tokenId = idToMarketplaceItem[itemId].tokenId;

        require(
            msg.value == price, 'the price is required for
            completing the purchase'
        );

        payable(owner).transfer(itemPrice);

        idToMarketplaceItem[itemId].seller.transfer(msg.value);
        IERC721(nftContract).transferFrom(address(this),
        msg.sender, tokenId);

        idToMarketplaceItem[itemId].owner = payable(msg.sender);
        idToMarketplaceItem[itemId].isSold = true;
        soldItems.increment();
    }
```

Figure 6.18: buyNft() Solidity function



Dystopian Utopia

PAINTINGS

Artist 0x70997970C51812d...

Seller 0x70997970C51812d...

2.5

USD 4875.05

Buy

Description

The gates of Valhalla, the Gardens of Babylon or the depths of the Atlantis

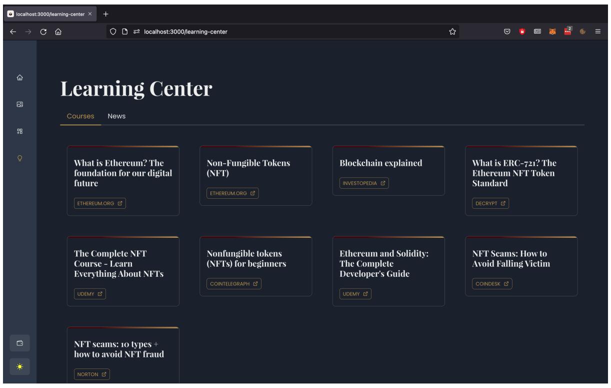
Figure 6.19: Smart NFT | Buy NFT from user page

Once an NFT item is available in the Marketplace, it is ready to be sold to other approved users. Consequently, a user can buy an asset by calling the `buyItem()` function from the smart contract with the NFT contract address and itemId as function arguments (fig. 6.18). The price and `tokenId` are derived and then, the exchange of assets is happening: if the buyer's wallet has enough funds, the NFT value in ETH is transferred to the seller wallet and the token is transferred from the seller to the buyer. Eventually, the `owner` property of the `MarketplaceItem` is being updated to match the buyer's wallet address and the item is maked as being sold with the `isSold` property.

On the user facing side, the process is straightforward, as the `BUY` button is present on an asset's dedicated page (fig. 6.19), on each NFT card displayed in the marketplace (fig. 6.6) and in the user's page (fig. 6.8), only when the item is purchasable by the authenticated user.

6.4.7 | Learning Center

While this is not a 'mission-critical' feature, as a response to the users' and experts' demands on educating the audience (sections 4.1, 4.2), the platform includes a 'Learning center' that contains links to reputable resources for learning about blockchain, NFTs and the entire cryptocurrencies ecosystem as a whole. In this way, it is possible to bring benefits both to the direct users, but also to the entire industry, as it is a method to raise awareness and increase trust in the ecosystem, in regards to the interested population.



localhost:3000/learning-center
localhost:3000/learning-center

Learning Center

Courses News

What is Ethereum? The foundation for our digital future — ETHEREUM.ORG

Non-Fungible Tokens (NFT) — ETHEREUM.ORG

Blockchain explained — INVESTOPEDIA

What is ERC-721? The Ethereum NFT Token Standard — DECRYPT

The Complete NFT Course - Learn Everything About NFTs — UDEMY

Nonfungible tokens (NFTs) for beginners — COINTELEGRAPH

Ethereum and Solidity: The Complete Developer's Guide — UDEMY

NFT Scams: How to Avoid Falling Victim — COINDESK

NFT scams: 10 types + how to avoid NFT fraud — NORTON

Figure 6.20: Smart NFT | List NFT

6.5 | Solution Evaluation

The set of features and functionalities described in the subsections above represent the main value points of the solution that has been developed. While they provide the functionalities required for the product to be considered an MVP, some implementation details and other smaller features have been deliberately left out from the section, in order to only consider the features with uttermost relevance. However, the system has included features for increased usability and ensuring users' safety when trading NFTs. In this perspective, it is possible to count extensive input validation, conditional rendering of pages or components that comprise authorised-only transactions and an enhanced focus on informing the user at any step about the state of their account or transactions.

Consequently, the functional prototype aims to address some of the flaws that are currently present in the ecosystem, as the enumerated findings conclude. This is done by leveraging the functionality that users' and experts have directly or indirectly expressed that was needed.

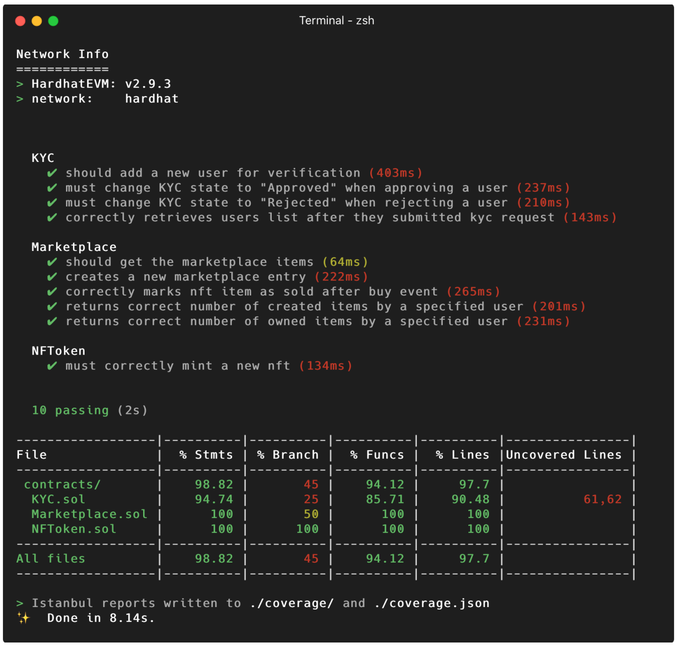
With the features and attributes it possesses, the MVP solution is ready to be tested against real prospective users, in order to gain the knowledge about the desirability of such a system and the eventual weaknesses that should be addressed in an upcoming iteration, as a consequence of the test results. Also, Appendices section C includes the installation instructions for the `Smart NFT` system, for allowing the user to test and interact with it in a secure and risk-free environment.

7 Testing

The following section relates the testing initiatives and frameworks that have been used for testing and Quality Assurance (QA), regarding the `Smart NFT` platform. The outcome of the section is represented by two different aspects. The first one is the requirements validation, where based on evidence and observations, the functional and non-functional requirements are quantified and assessed whether they have successfully been implemented. The second aspect consists in extracting valuable feedback (especially from the conducted user testing) that would constitute the basis for a new iteration of the system.

7.1 | Software/Unit Tests

In the software development field, testing a system before release is an industry standard, as it prevents unfortunate errors and bugs from being experienced by end users [81]. Some businesses or institutions take this one step further by implementing Test-Driven Development, or TDD, where tests are written prior to the code implementation, followed by constantly running and failing them, and gradually writing the code that will make them pass [82].



```
Network Info
============
> HardhatEVM: v2.9.3
> network:    hardhat



  KYC
    ✔ should add a new user for verification (403ms)
    ✔ must change KYC state to "Approved" when approving a user (237ms)
    ✔ must change KYC state to "Rejected" when rejecting a user (210ms)
    ✔ correctly retrieves users list after they submitted kyc request (143ms)

  Marketplace
    ✔ should get the marketplace items (64ms)
    ✔ creates a new marketplace entry (222ms)
    ✔ correctly marks nft item as sold after buy event (265ms)
    ✔ returns correct number of created items by a specified user (201ms)
    ✔ returns correct number of owned items by a specified user (231ms)

  NFToken
    ✔ must correctly mint a new nft (134ms)


  10 passing (2s)

------------------|----------|----------|----------|----------|----------------|
File              |  % Stmts | % Branch |  % Funcs |  % Lines |Uncovered Lines |
------------------|----------|----------|----------|----------|----------------|
 contracts/       |    98.82 |       45 |    94.12 |     97.7 |                |
  KYC.sol         |    94.74 |       25 |    85.71 |    90.48 |          61,62 |
  Marketplace.sol |      100 |       50 |      100 |      100 |                |
  NFToken.sol     |      100 |      100 |      100 |      100 |                |
------------------|----------|----------|----------|----------|----------------|
All files         |    98.82 |       45 |    94.12 |     97.7 |                |
------------------|----------|----------|----------|----------|----------------|

> Istanbul reports written to ./coverage/ and ./coverage.json
✨  Done in 8.14s.
```

Figure 7.1: Smart NFT | Unit tests output

In the current case, the scale, scope and the relatively short time frame of the project did not allow for an extensive test coverage for the entire code base. However, the focus was to test the critical components within the system, which are represented by the smart contracts. Each of the three smart contracts comes with a set of functions that are called from the client, as illustrated in section 6. Consequently, the most relevant testing method for the smart contracts was writing unit tests that help in assessing whether the functions are performing correctly.

By running the test utility, it is possible to observe that all the tests have passed and there is a test coverage of 98.82% among all the three smart contract files, as seen in figure 7.1. With this percentage in place, the tested smart contracts can comfortably be trusted that they are executing correctly.

7.2 | User testing

In order to objectively assess the effectiveness of the `Smart NFT` platform as a 'tangible' solution to the NFT ecosystem current state and problem area, user and usability testing have been merged and conducted in the shape of a think-aloud protocol, based on a list of predefined tasks. It is necessary to state that user testing in essence refers to measuring the extent to which a given product or system is needed or desired by the users, while usability testing consists in measuring and assessing how easy it is for a user to use a system and what are the potential weaknesses that it has [83].

Merging the two approaches was decided for obtaining the feedback that would prove valuable both in terms of validating the solution desirability and contributing to an improved version to be built in a further iteration.

7.2.1 | Testing Methodology

A number of five respondents have been selected from the author's network and one selection criteria was having at least a basic understanding or minimal contact with the blockchain or cryptocurrencies field. This was to test that the solution could cater to actual prospective users' needs.

For ensuring efficiency and effectiveness, the user testing has been conducted remotely and synchronously, by using tools as Google Meet for video communication and TeamViewer for remote access. While the current section highlights the key takeaways, the specific notes and observations can be found in the Appendices section B.

7.2.2 | Evaluation Technique

For obtaining both qualitative and quantitative results, each task was assigned a complexity score that denotes the degree of difficulty encountered when attempting to complete it. The score range was from 1 to 5, where 1 stands for 'effortless' and 5 stands for 'highly demanding'. This is documented under each question in the shape of a histogram featuring the mean value. Further, the most relevant user observations have been noted as a part of the qualitative findings and insights, while the similar thoughts have been filtered out.

Due to the fact that the users have tested the system on a localhost network while remotely accessing the author's machine, it was a prerequisite to be authenticated in a demo wallet instance with a non-null ETH balance. In this way, the users were prevented from connecting with their own wallet and eventually from using a mainnet with real funds. Accordingly, the given tasks are based on the assumption that the user has already connected their crypto wallet to the dApp. Consequently, users were informed about this and about the fact that any spent funds are testnet ETH with no inherent value, prior to starting the sessions.

7.2.3 | Results

The initial task of navigating to a user's profile from the marketplace page was easily performed by all the participants, the mean of the complexity score being 1.4, specific to a complexity level between effortless and easy. Users have also appreciated the usage of meaningful icons for the side navigation bar, but for those who have not traded cryptocurrencies so far, they would appreciate if the name of the user was rendered next to the avatar instead of the wallet address.

Furthermore, on the task of submiting the KYC verification request form, most of the users have righteously raised concerns over how the submitted data was going to be stored and used, as they were not aware of the data encryption mechanism employed before storing it on-chain. Still, a learning outcome is that users must be made aware of the privacy policy, in order to prevent any concerns about the topic. Besides this, one of the users with no prior cryptocurrency trading experience stated that she was not aware of having to pay network fees for submitting a form. However, this is a standard operation for any blockchain-related transaction, as the submitted data was being stored on the DLT and not on a centralised server, so it automatically included the network fees required for it. The complexity mean of this task was 1.8.

Moreover, the task of purchasing an NFT proved to be quite straightforward for the majority of the participants, especially after having the initial experience of interacting with the Metamask wallet for approving a transaction. With a complexity mean of 1.6, the key takeaways from the verbal user feedback are that users need to be made aware of the fact that they are going to engage in an irreversible transaction, since the process could possibly have been too fast.

Nevertheless, the task of finding the newly purchased NFT in the user interface gained a complexity mean of 1.2, as it was straightforward for all the users, since they were already redirected to their own user page after purchasing it. Consequently, they only had to navigate to the right tab within the page. Also, the last task of uploading and listing a new NFT obtained a complexity mean of 1.6. The received feedback was positive towards the real-time price convertion of ETH to USD, and the straightforward process of minting and listing the NFT. One concern was raised though, in regards to the necessity of approving two transactions in Metamask. However, this was also natural to happen, as the first transaction was the NFT minting, while the second was listing it on the marketplace.

Overall, the user and usability test revealed a well performing system, with a promising overall complexity mean of 1.52 and no cases of major difficulties in completing any of the given tasks. Besides this, all users have expressed the willingness to use such a platform in a real scenario, if their submitted KYC data was stored and used in a secure manner, because the verification aspect offers an extra layer of assurance. However, one more desired feature that was exposed by some participants was the content curation aspect, as it would contribute to a more trustworthy ecosystem. Consequently, the `Smart NFT` solution has successfully been validated and the relevant learning have been included in the backlog as tasks for the next product iteration.

7.3 | Requirements Validation

After successfully running the unit tests on the smart contracts and the user/usability testing, it was possible to conduct the requirements validation process, that enabled an objective perspective on the state of the system requirements and to what extent they have actually been implemented.

Consequently, the ratio was corresponding to 88.24% coverage of validated requirements, with only 4 out of 34 not being implemented. The reasons for that were related to narrowing the scope of the project (as exposed in the Delimitations section 1.2), in the case of functional requirements 14, 15 and non-functional requirements 18 and 19.

ID	Functional Requirement	Validation
1	The system must consist in a decentralised front-end application connecting to a smart contract interface.	true
2	The user must be able to connect their crypto wallet browser extension to the system.	true
3	The system must allow all users to browse through an NFT marketplace.	true
4	The system must allow all users access to a Learning centre including links to reputable resources for educating the audience and to crypto-related news articles.	true
5	The system must allow all users to view all metadata related to NFT listings.	true
6	The system must allow all users to view the partial profiles of verified users that include the set of NFTs that they created, sold and owned.	true
7	The system must allow users who have connected their crypto wallets to submit a KYC verification request form.	true
8	The system must encrypt sensitive user data sent within the KYC request form.	true
9	The system must allow authenticated *admin* user types to decrypt sensitive user data for verification purposes.	true
10	The authenticated *admin* user type must be able to approve or reject a user's KYC request form.	true
11	The approved user must be able to mint an NFT.	true
12	The approved user must be able to buy an NFT.	true
13	The approved user must be able to sell an NFT.	true
14	The approved user should be able to access a personalised dashboard containing the historical values of their NFT portfolio and trading KPIs.	false
15	The system could require content curation before NFT assets are listed on the public marketplace.	false

Table 7.1: Functional Requirements Validation

ID	Non-Functional Requirement	Validation
1	The system must use the Polygon blockchain network with Solidity smart contracts as the underlying decentralised layer.	true
2	The system must embed a NextJS front-end application that is able to call smart contract functions via a third party NodeJS library.	true
3	The system must support connections to the Metamask browser wallet extension.	true
4	The system must store NFT assets on the Polygon network and the corresponding file metadata using the decentralised IPFS protocol, for preserving data integrity.	true
5	The system must display the ownership structure and origin of each listed NFT asset, as the wallet addresses of the creators and owners, linked to the corresponding user profiles.	true
6	The system must include a KYC verification request form that must be accessible by users with connected crypto wallets, but who did not previously submit the form.	true
7	The KYC verification form must adhere to and follow the general standards and questions that are usually addressed in banking institutions' KYC processes.	true
8	The system must use the AES symmetric encryption algorithm to encrypt sensitive user data sent with the KYC request form before storing it on-chain, in an immutable format.	true
9	The system must store files added as documentation during the KYC process using the IPFS protocol, for preventing tampering with their metadata.	true
10	The system must generate user profiles for the users who have successfully submitted the KYC verification request form.	true
11	The KYC smart contract must provide a getter function for fetching the list of users who have submitted a KYC request, that is only callable by admin user types.	true
12	The system must provide the admin user types with the secret key for decrypting the submitted sensitive user data, for verification purposes.	true
13	The KYC smart contract must employ functions for approving or rejecting a KYC request that are only callable by admin user types.	true
14	The system must feature an ERC-721 compliant smart contract for minting non-fungible tokens on the Polygon network, that is only accessible by approved users.	true
15	The system must employ a marketplace smart contract that provides functions for buying and selling NFT assets, that are only callable by approved users.	true
16	The system must support ETH on the Polygon network as the cryptocurrency of choice for increased performance and reduced network fees.	true
17	The front-end application must re-use components from a GUI components library, for enabling an understandable and easy to use flow for the end users.	true
18	The front-end application should compute the sales volume and purchases related to a user for displaying a visual overview of the users' transactions and history.	false
19	The system won't employ computer vision ML algorithms to verifying the user submissions, and curating them before approving them and publishing them on the platform.	false

Table 7.2: Non-Functional Requirements Validation

8 Discussion

Throughout the course of the project, it was possible to obtain relevant findings from trusted resources, that helped in shaping a holistic and comprehensive solution to the stated research question. The project work was structured by following an adapted version of the SCRUM process model [30] on top of the Design Thinking Process methodology [33], comprising five steps, as described in subsection 2.4. The process followed an iterative and incremental approach, both in terms of thesis writing and software development.

As the area of interest revolved around NFTs and digital collectibles - a modern and advanced concept powered by blockchain technology, the first natural step was to conduct a Literature review for discovering and analysing existing scientific literature on the topic (section 3.1). Some of the key findings extracted from the literature review revealed the existing gaps in the NFT ecosystem, in terms of acknowledging the real creators of digital artwork. This is because the current state of the ecosystem is based on the assumption that users submitting their creations as NFTs on specialised platforms are who they claim to be. This was one of the first indicators that the ecosystem was lacking a proper verification method for NFT traders.

Furthermore, the State of the Art (section 3) continued with an overview of the technological enablers that were initially considered and subsequently used in the development of the `Smart NFT` functional prototype. Among the analysed and used technologies, it is possible to count the Polygon Layer 2 blockchain, the ERC-721 standard for NFT smart contracts and the IPFS protocol for storing files and their metadata in a decentralised fashion.

In addition, the analysis of the case studies led to revealing more of the hands-on challenges that existing marketplaces were facing, such as hosting a high rate of counterfeit NFT assets [61], being investigated for violation of the U.S. securities law [65] or only supporting blockchains with scalability issues (eg. requiring soaring amounts in gas fees) [66]. Such issues have been addressed by the developed functional prototype, as for example, the Polygon blockchain that is built upon uses a scalable PoS consensus mechanism and incurs low gas fees. Also, unlike OpenSea, `Smart NFT` only allows hosting NFT associated files on the IPFS network, fact that makes it more resilient and provides data integrity.

Furthermore, the State of the Art section allowed for planning and conducting data collection (expert interviews and a user survey) by preparing appropriate questions and addressing them to a relevant segment of population (sections 4.1, 4.2). By doing so, it was possible to obtain genuine feedback from both potential users and experts within the field, which was subsequently used especially for drafting the use case diagrams (5.1.3) and then, the sets of functional and non-functional requirements for the delivered system (5.2). The main findings from the primary data collection section included the need for extra security measurements, mechanisms and even embedded user verification, in order to allow even users who potentially positioned themselves against cryptocurrencies, to trust more the NFT ecosystem. However, experts highlighted that there was also a need for educating the audiences and making them more aware about the volatile ecosystem that they were part of.

All these data points formed the prerequisites of the given solution, which was incrementally engineered within the Ideation process (identifying personas, scenarios and use case diagrams) and the Requirements specification 5.2. While the functional prototype is just the 'tangible' demonstration of the concept, the essential outcome of the project is represented by the findings about what makes a decentralised NFT trading platform a more secure place, where users can trust the authenticity of the listed NFT assets.

The results of the study conclude that such a platform should embed a mandatory KYC verification process for users who would like to engage in trading NFTs, that would ideally be accompanied by a thorough curation of the submissions before they are publicly listed. Besides that, it was demonstrated that even users who previously had contact with the cryptocurrencies field need access to learning resources about NFTs, to be able to take reponsible decisions when getting involved in trading.

8.1 | Limitations

When reflecting about the limitations that affected the course of the current project, it is possible to count the narrow time span allocated, which consisted in approximately four months. While it was possible to fit the research process within the given time span, building a functional prototype implied some trade-offs between roughly serving its given purpose and providing a seamless user experience, with smooth interactions. In this regards, the prototype is not a fully fledged production-ready system, but it proved to be a solid MVP that was capable of validating the product and achieving the purpose it was engineered for.

Moreover, with the NFT field being still in its infancy, the amount of scientific papers, articles or especially books on the topic is scarce. In the beginning of the project, this was considered as a significant limitation that could have hindered the ability to obtain enough valuable secondary data from academic resources. However, the Literature review section (3.1) included several scientific papers that proved to be sufficiently valuable in the development of the project.

Last but not least, Web3 software development is a highly demanding and resource-intensive process, so one limitation that affected the course of the project was represented by the need to allocate additional time to consult Web3 development learning resources, including Solidity courses and documentation sites of the used libraries. Hence, this automatically incurred less time for actual development work, so the functional prototype does not include performance optimisations and other usability tweaks. However, the essential pieces of functionality that it was built for are stable, unit-tested and ready to use, at least in a testnet environment.

9 Conclusion

NFTs are and will likely continue to be a leading area of interest within the blockchain and crypto ecosystem, in the near future and possibly for longer. With the current unregulated state and massive amount of fraud and counterfeiting happening in the industry, the current study aimed to address these challenges with a solution based on decentralised authentication mechanisms and KYC verification processes.

To clearly define the solution, it is necessary to reiterate the research question:

How can blockchain technology aid in certifying the authenticity of NFT digital artwork so that art investors can trust the value of their investment?

Accordingly, the solution for it primarily consists of a decentralised NFT marketplace featuring advanced user verification mechanisms, based on an enhanced KYC process inspired by the traditional financial ecosystem, as described in section 6.1. Subsequently, for ensuring complete transparency and decentralisation, the KYC user data is stored on-chain, which means that it is possible to have a persistent storage of the user details and the NFT assets that they are minting and/or trading. Also user privacy is a prime concern, and since a KYC form requests sensitive personal information, the data needs to be encrypted before being stored immutably on the ledger, authorising only the system administrators (most likely compliance agents) access to the decryption key.

For also addressing the initial sub-question (from subsection 1.1.1), it is necessary to state that blockchain technology provides benefits such as immutability and irreversibility of transactions [9]. This ensures the non-repudiation software quality, so no transaction can be denied by its issuer. Moreover, smart contract addresses are unique, and only by verifying the address of the smart contract (eg. on Etherscan, Polygonscan) of an NFT item, an investor can ensure that it is the actual NFT that they want to interact with.

When considering the second sub-question, an authentication mechanism that is binding a wallet address to a KYC verified user account contributes to certifying the authenticity of a user, initially, and also of the assets that they create, since users who go through a KYC process are less likely to be able to commit fraud and submit counterfeit entries without being identified and possibly prosecuted. The wallet address would then be used as an identifier for the authenticated user, as the prerequisite to perform minting, buying or selling transactions is to connect a wallet to the system that is appended to a user who has passed the KYC verification process. Another relevant mechanism that would provide an extra layer of security would be curating the NFT submissions, either through manual labour or AI algorithms for tracking occurrences of digital artwork and their copies, both on the platform and on the Internet.

Nevertheless, the third sub-question relates to the marketplaces' liability for the stored user generated content. While regulatory frameworks are yet to be implemented, marketplaces are not legally bound to curate any of the hosted content. However, the NFT and crypto ecosystem should not wait for regulation to be implemented. For keeping the momentum, it is mandatory to enable trust on the users side, and therefore, platforms should enforce all measures for preventing their users from being victims of cyber attacks, theft or fraud. This includes basic features like explicitly displaying the NFTs and users contract addresses, linking them to the blockchain scanner pages of the addresses and more importantly, educating the users about blockchain and about how NFTs work.

As findings from the the expert interviews state, it is not (yet) illegal to reuse the same media file from a listed NFT, because there are no copyrights appended to NFTs [84]. In this sense, the uniqueness of an NFT stands in the digital hash stored on the blockchain, rather than the attached image or media file. While this is something that the users should be informed about, in the first place, a platform should still have internal policies to prevent and detect such cases, so users are less likely to purchase the NFT linked to the 'copy' of a genuine media file, at least for ethical purposes. This is something to consider at least until copyrights could become part of NFT assets, as well.

All of the aforementioned findings have concretely been demonstrated by the 'tangible' outcome of the project, which is the `Smart NFT` functional prototype that encompasses the described features. In this perspective, the prototype has been validated with user and usability testing, and it represents a solid foundation for a fully-fledged system that could have the potential to increase the NFTs adoption rate at a global scale.

9.1 | Future Perspectives

This section aims to reflect on eventual further improvements that the functional prototype should embed, starting from the Requirements validation section (7.3) and the feedback retrieved from the conducted usability testing (7.2).

A usability improvement inferred from the unvalidated requirements is to include a personalised dashboard for authenticated and verified users, that would showcase trading statistics and KPIs (Key Performance Indicators), that would perform computation of data retrieved directly from the DLT. This would allow the user to have an overview of a history of transactions and value of purchased and sold NFTs.

Another improvement that would add an extra layer of security is to extend the system with an AI-powered content curation service, that would crawl the Internet for tracking occurrences of the same or similar media files. This would help reinforcing the users' confidence that the contract they interact with is corresponding to the first producer of a specific media file.

Moreover, the existing KYC process would benefit from an optimisation enhancement. Due to the amount of data that is currently stored on-chain, transaction gas fees can become rather expensive. For improving this aspect, it is possible to reduce number of the smart contract function arguments and the number of added characters as well. This can be pursued by mapping for example, NFT category names to bucket IDs that can be stored on-chain for a less cost.

Other usability improvements refer to the front-end of the system and include the state updates being able to trigger component re-renders instead of page reloads and moreover, adding more focus on educating the audiences. Besides the already existing Learning Center, a quick start guide could be added, that should describe a complete flow for using the platform. Moreover, the user should at all times be warned with disclaimers before engaging in a transaction, for ensuring that the user knows the risks that they expose to while trading NFTs.

Lastly, improving the wallet authentication process has been in question, especially by considering Two factor authentication. However, Metamask is a non-custodial wallet, meaning that it does not store any of the wallet data or the seed phrase and therefore, has no access or control of the user keys [85]. For this reason, Two factor authentication is not compatible with non-custodial wallets and has been excluded from the list of possible further improvements. Still, in the crypto ecosystem, the choice of a non-custodial wallet is widely considered more secure than a custodial wallet that employs Two factor authentication [85].

9.2 | Contribution to Knowledge

One of the main contributions to knowledge and to the academic environment is represented by the validation of the functional prototype within the conducted user testing. In this way, the need for a secure context for trading NFTs has been acknowledged and it is likely that more steps in this direction will be taken by the industry leaders.

Moreover, since an integral part of the solution comprises educating the audiences interested in the cryptocurrencies and NFT field, the information illustrated in the current thesis addresses exactly this need. One of the most valuable obtained insights is the separation between the unique hash stored on-chain representing the actual NFT and the media file that it is connected to.

Additionally, the thesis presents a significant contribution to the academic space, as the number of valuable research papers on the topic is relatively low, at the time of writing. Also, currently with no business entities implementing the authentication and KYC mechanisms described above, the thesis aims to pioneer the approach and to open the path towards enhancing the NFT industry and making it a more secure space for trading digital assets, both for creators and for investors.

Bibliography

[1] J. Mokyr and R. H. Strotz. “The second industrial revolution, 1870-1914”. In: *Storia dell’economia Mondiale* 21945.1 (1998).

[2] I. Bojanova. “The digital revolution: what’s on the horizon?” In: *IT Professional* 16.1 (2014), pp. 8–12.

[3] Bitdeal. *Enterprise Blockchain Solutions.* Accessed: 2022-03-17. URL: `https://www.bitdeal.net/`.

[4] T. O’reilly. *What is web 2.0.* O’Reilly Media, Inc., 2009.

[5] R. Hawkins. “Looking beyond the dot com bubble: exploring the form and function of business models in the electronic marketplace”. In: *E-life after the dot com bust.* Springer, 2004, pp. 65–81.

[6] *Number of internet users worldwide from 2005 to 2021.* Accessed: 2022-02-18. URL: `https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/`.

[7] R. King. *Web3: The hype and how it can transform the internet.* Accessed: 2022-02-18. Feb. 1, 2022. URL: `https://www.weforum.org/agenda/2022/02/web3-transform-the-internet/`.

[8] G. Edelman. *The Father of Web3 Wants You to Trust Less.* Accessed: 2022-02-18. Nov. 29, 2021. URL: `https://www.wired.com/story/web3-gavin-wood-interview/`.

[9] *Time for trust: How blockchain will transform business and the economy.* Accessed: 2022-02-27. URL: `https://www.pwc.com/gx/en/industries/technology/publications/blockchain-report-transform-business-economy.html`.

[10] Q. Wang et al. “Non-fungible token (NFT): Overview, evaluation, opportunities and challenges”. In: *arXiv preprint arXiv:2105.07447* (2021).

[11] T. Locke. *Jack Dorsey sells his first tweet ever as an NFT for over $2.9 million.* Accessed: 2022-03-07. Mar. 22, 2021. URL: `https://www.cnbc.com/2021/03/22/jack-dorsey-sells-his-first-tweet-ever-as-an-nft-for-over-2point9-million.html`.

[12] C. Bumbaca. *LeBron James NBA Top Shot moment of dunk honoring Kobe Bryant auctions for $387,600.* Accessed: 2022-03-07. Apr. 16, 2021. URL:

https://eu.usatoday.com/story/sports/nba/lakers/2021/04/16/lebron-james-nba-top-shot-moment-auction/7251326002/.

[13] I. Lee. *Sales of Bored Ape Yacht Club NFTs jump past $1 billion amid heightened interest from celebrity collectors.* Accessed: 2022-03-07. Jan. 4, 2022. URL: https://markets.businessinsider.com/news/currencies/bored-ape-yacht-club-nft-sales-1-billion-opensea-bayc-2022-1.

[14] T. Akhtar. *Investor Gary Vaynerchuk Says NFTs Are Like the Dot-Com Bubble.* Accessed: 2022-03-07. Mar. 16, 2021. URL: https://www.coindesk.com/markets/2021/03/16/investor-gary-vaynerchuk-says-nfts-are-like-the-dot-com-bubble/.

[15] E. Howcroft. *Unreal demand? Irregular sales worth billions fire up wild NFT market.* Accessed: 2022-02-27. Feb. 7, 2022. URL: https://www.reuters.com/technology/unreal-demand-irregular-sales-worth-billions-fire-up-wild-nft-market-2022-02-07/.

[16] A. Krion. *NFT Regulation Looms Large, So Let's Start With the Proper Framework.* Accessed: 2022-02-17. Nov. 9, 2021. URL: https://www.nasdaq.com/articles/nft-regulation-looms-large-so-lets-start-with-the-proper-framework.

[17] J. Pearson. *More Than 80% of NFTs Created for Free on OpenSea Are Fraud or Spam, Company Says.* Accessed: 2022-03-19. Jan. 28, 2022. URL: https://www.vice.com/en/article/wxdzb5/more-than-80-of-nfts-created-for-free-on-opensea-are-fraud-or-spam-company-says.

[18] L. Bakare. *Collector buys fake Banksy NFT for £244,000.* Accessed: 2022-03-17. Sept. 1, 2021. URL: https://www.theguardian.com/technology/2021/sep/01/collector-buys-fake-banksy-nft-for-244000.

[19] E. Genç. *Investors Spent Millions on 'Evolved Apes' NFTs. Then They Got Scammed.* Accessed: 2022-03-17. Oct. 5, 2021. URL: https://www.vice.com/en/article/y3dyem/investors-spent-millions-on-evolved-apes-nfts-then-they-got-scammed.

[20] V. Alexiev. *NFTs and the Dawn of the Metaverse.* Accessed: 2022-03-16. Apr. 6, 2021. URL: https://www.citi.com/ventures/perspectives/opinion/nfts-metaverse.html.

[21] P. A. Clark. *The Metaverse Has Already Arrived. Here's What That Actually Means.* Accessed: 2022-03-19. Nov. 15, 2021. URL: https://time.com/6116826/what-is-the-metaverse/.

[22] *Cryptocurrency users worldwide 2021 | Statista.* Accessed: 2022-02-17. URL: https://www.statista.com/statistics/1202503/global-cryptocurrency-user-base/.

[23] A. Hayes. *Blockchain Explained.* Accessed: 2022-03-19. Mar. 5, 2022. URL: https://www.investopedia.com/terms/b/blockchain.asp.

[24] K. B. Wilson, A. Karg, and H. Ghaderi. “Prospecting non-fungible tokens in the digital economy: Stakeholders and ecosystem, risk and opportunity”. In: *Business Horizons* (2021).

[25] Investopedia. *Fungibility Definition.* Accessed: 2022-03-19. URL: https://www.investopedia.com/terms/f/fungibility.asp.

[26] *Digital Art.* Accessed: 2022-03-19. URL: https://www.tate.org.uk/art/art-terms/d/digital-art.

[27] B. Powers. *Scams and Fraud Bubble Up as NFT Mania Takes Hold.* Accessed: 2022-02-17. Mar. 31, 2021. URL: https://www.coindesk.com/tech/2021/03/31/scams-and-fraud-bubble-up-as-nft-mania-takes-hold/.

[28] K. Schwaber and M. Beedle. *Agile software development with Scrum.* Vol. 1. Prentice Hall Upper Saddle River, 2002.

[29] K. Schwaber and J. Sutherland. “The scrum guide”. In: *Scrum Alliance* 21.1 (2011).

[30] *SCRUM Framework.* Accessed: 2022-03-20. URL: https://www.scrum.org.

[31] W. G. Axinn and L. D. Pearce. *Mixed method data collection strategies.* Cambridge University Press, 2006.

[32] R. F. Dam and T. Y. Siang. *What is Design Thinking and Why Is It So Popular?* Accessed: 2022-03-24. 2021. URL: https://www.interaction-design.org/literature/article/what-is-design-thinking-and-why-is-it-so-popular.

[33] *5 Stages in the Design Thinking Process.* Accessed: 2022-03-24. URL: https://www.interaction-design.org/literature/article/5-stages-in-the-design-thinking-process.

[34] S. Gibbons. *Design Thinking 101.* Accessed: 2022-03-24. July 31, 2016. URL: https://www.nngroup.com/articles/design-thinking/.

[35] J. Smith. “Is ’State of the Art’ Patently Ill Defined?” In: (1988). Accessed: 2022-03-27. URL: https://www.latimes.com/archives/la-xpm-1988-06-15-vw-4099-story.html.

[36] M. McConaghy et al. “Visibility and digital art: Blockchain as an ownership layer on the Internet”. In: *Strategic Change* 26.5 (2017), pp. 461–470.

[37] M. Zeilinger. “Digital art as ‘monetised graphics’: Enforcing intellectual property on the blockchain”. In: *Philosophy & Technology* 31.1 (2018), pp. 15–41.

[38] U. W. Chohan. “Non-fungible tokens: Blockchains, scarcity, and value”. In: *Critical Blockchain Research Initiative (CBRI) Working Papers* (2021).

[39] L. Kohnfelder and P. Garg. “The threats to our products”. In: *Microsoft Interface, Microsoft Corporation* 33 (1999).

[40] *State of the DApps - DApp Statistics.* Accessed: 2022-03-27. URL: https://www.stateofthedapps.com/stats/.

[41] *Solidity 0.8.13 Documentation.* Accessed: 2022-03-27. URL: https://docs.soliditylang.org/en/v0.8.13/.

[42] *Ethereum development documentation | ethereum.org*. Accessed: 2022-03-27. URL: https://ethereum.org/en/developers/docs/.

[43] A. Narayanan et al. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press, 2016.

[44] J. Sedlmeir et al. "The energy consumption of blockchain technology: beyond myth". In: *Business & Information Systems Engineering* 62.6 (2020), pp. 599–608.

[45] J. Redman. *Average Ethereum Gas Fee Jumps to $20 per Transfer, L2 Fees Follow Rise*. Accessed: 2022-04-03. Apr. 3, 2022. URL: https://news.bitcoin.com/average-ethereum-gas-fee-jumps-20-per-transfer-l2-fees-follow-rise/.

[46] E. Oosterbaan. *Why Ethereum's 'Difficulty Bomb' Has Been Delayed Again*. Accessed: 2022-04-03. Dec. 15, 2021. URL: https://www.nasdaq.com/articles/why-ethereums-difficulty-bomb-has-been-delayed-again.

[47] D. Phillips. *What is Polygon (MATIC) and Why It Matters for Ethereum*. Accessed: 2022-04-03. Mar. 11, 2021. URL: https://decrypt.co/resources/what-is-polygon-matic-and-why-it-matters-for-ethereum.

[48] *Polygon Technology | Documentation*. Accessed: 2022-04-03. URL: https://docs.polygon.technology/.

[49] S. Casale-Brunet et al. "Networks of Ethereum Non-Fungible Tokens: A graph-based analysis of the ERC-721 ecosystem". In: *2021 IEEE International Conference on Blockchain (Blockchain)*. IEEE. 2021, pp. 188–195.

[50] *ERC-721 Non-Fungible Token Standard — ethereum.org*. Accessed: 2022-03-27. URL: https://ethereum.org/en/developers/docs/standards/tokens/erc-721/.

[51] *EIP-721: Non-Fungible Token Standard*. Accessed: 2022-04-03. URL: https://eips.ethereum.org/EIPS/eip-721.

[52] *ERC-1155 Multi-Token Standard — ethereum.org*. Accessed: 2022-04-03. URL: https://ethereum.org/en/developers/docs/standards/tokens/erc-1155/.

[53] D. Hays et al. *Nonfungible Tokens: A New Frontier*. Accessed: 2022-04-03. 2021. URL: https://research.cointelegraph.com/reports/detail/ckze3t71j00stftpd4yxg4xss.

[54] K. R. Lakhani and M. Iansiti. "The truth about blockchain". In: *Harvard Business Review* 95.1 (2017), pp. 119–127.

[55] *IPFS Documentation | IPFS Docs*. Accessed: 2022-04-03. URL: https://docs.ipfs.io/.

[56] C. Dupres. *IPFS, Filecoin and the Long-Term Risks of Storing NFTs*. Accessed: 2022-04-03. Jan. 20, 2022. URL: https://www.coindesk.com/layer2/2022/01/20/ipfs-filecoin-and-the-long-term-risks-of-storing-nfts/.

[57] *OpenSea, the largest NFT marketplace.* Accessed: 2022-04-06. URL: https://opensea.io/.

[58] S. Ehrlich. *NFT Marketplace CEO Explains Why The Industry Is Moving Beyond Ideological Purists.* Accessed: 2022-04-06. July 6, 2021. URL: https://www.forbes.com/sites/stevenehrlich/2021/07/06/nft-marketplace-ceo-explains-why-the-industry-is-moving-beyond-ideological-purists/.

[59] A. Atallah. *Decentralizing NFT metadata on OpenSea.* Accessed: 2022-04-06. June 17, 2021. URL: https://opensea.io/blog/announcements/decentralizing-nft-metadata-on-opensea/.

[60] *Biggest NFT marketplaces 2021 | Statista.* Accessed: 2022-04-06. URL: https://www.statista.com/statistics/1274843/nft-marketplaces-with-highest-volume/.

[61] *OpenSea on Twitter.* Accessed: 2022-04-06. Mar. 14, 2021. URL: https://twitter.com/opensea/status/1370895902982946820.

[62] G. M. Volpicelli. *NFT Marketplace CEO Explains Why The Industry Is Moving Beyond Ideological Purists.* Accessed: 2022-04-06. Feb. 10, 2022. URL: https://www.wired.com/story/opensea-nfts-twitter/.

[63] R. Brandom. *$1.7 million in NFTs stolen in apparent phishing attack on OpenSea users.* Accessed: 2022-04-06. Feb. 20, 2022. URL: https://www.theverge.com/2022/2/20/22943228/opensea-phishing-hack-smart-contract-bug-stolen-nft/.

[64] *Home | Fractional.* Accessed: 2022-04-07. URL: https://fractional.art/.

[65] M. Robinson. *SEC Scrutinizes NFT Market Over Illegal Crypto Token Offerings.* Accessed: 2022-04-07. Mar. 2, 2022. URL: https://www.bloomberg.com/news/articles/2022-03-02/sec-scrutinizes-nft-market-over-illegal-crypto-token-offerings.

[66] L. Matney. *NFT art marketplace SuperRare closes $9 million Series A.* Accessed: 2022-04-07. Mar. 30, 2021. URL: https://techcrunch.com/2021/03/30/nft-art-marketplace-superrare-closes-9-million-series-a/.

[67] *SuperRare | NFT Art | NFT Art Marketplace | Digital Art.* Accessed: 2022-04-07. URL: https://superrare.com/.

[68] M. Aoyama. “Persona-and-scenario based requirements engineering for software embedded in digital consumer products”. In: *13th IEEE International Conference on Requirements Engineering (RE’05)*. IEEE. 2005, pp. 85–94.

[69] I. Sommerville. “Software engineering 9th Edition”. In: (2011).

[70] P. Eeles. *What, no supplementary specification?* Accessed: 2022-05-07. July 31, 2016. URL: https://web.archive.org/web/20201111213648/https://www.ibm.com/developerworks/rational/library/3975.html.

[71] Investopedia. *Know Your Client (KYC) Definition.* Accessed: 2022-05-07. URL: https://www.investopedia.com/terms/k/knowyourclient.asp.

[72] G. E. Krasner, S. T. Pope, et al. “A description of the model-view-controller user interface paradigm in the smalltalk-80 system”. In: *Journal of object oriented programming* 1.3 (1988), pp. 26–49.

[73] *Getting Started | Next.js.* Accessed: 2022-05-10. URL: https://nextjs.org/docs/getting-started.

[74] *Polygon PoS - Infura Docs.* Accessed: 2022-05-10. URL: https://docs.infura.io/infura/networks/polygon-pos.

[75] *Overview | Hardhat | Ethereum development environment for professionals by Nomic Foundation.* Accessed: 2022-05-12. URL: https://hardhat.org/getting-started/.

[76] *Introduction | MetaMask Docs.* Accessed: 2022-05-10. URL: https://docs.metamask.io/guide/.

[77] *Introduction - Chai.* Accessed: 2022-05-10. URL: https://www.chaijs.com/api/.

[78] *Ethers Documentation.* Accessed: 2022-05-10. URL: https://docs.ethers.io/v5/.

[79] *TypeScript: Documentation.* Accessed: 2022-05-10. URL: https://www.typescriptlang.org/docs/handbook/.

[80] *First Steps - Chakra UI.* Accessed: 2022-05-10. URL: https://chakra-ui.com/guides/first-steps.

[81] B. Hailpern and P. Santhanam. “Software debugging, testing, and verification”. In: *IBM Systems Journal* 41.1 (2002), pp. 4–12.

[82] K. Beck. *Test-driven development: by example.* Addison-Wesley Professional, 2003.

[83] J. S. Dumas, J. S. Dumas, and J. Redish. *A practical guide to usability testing.* Intellect books, 1999.

[84] A. Guadamuz. *What do you actually own when you buy an NFT?* Accessed: 2022-05-23. Feb. 7, 2022. URL: https://www.weforum.org/agenda/2022/02/non-fungible-tokens-nfts-and-copyright/.

[85] G. Goodell, H. D. Al-Nakib, and P. Tasca. “A Digital Currency Architecture for Privacy and Owner-Custodianship”. In: *Future Internet* 13.5 (2021), p. 130.

Appendices

A Primary Data Sources

A.1 | Expert Interviews

Description

The purpose of the expert interviews is to understand what is missing from a technical perspective and what could be done further in order to prevent malicious activity as cyber theft and counterfeits in the NFT industry.

Participants

- **Christian Carle**, Social Support Specialist at Voyager Digital LLC. (VYGVF)
- **Anonymous Respondent**, Senior Software Engineer at *Undisclosed Company*

Disclaimer

All of the the opinions expressed in the interviews are those of the respondents. They do not purport to reflect the opinions or views of their employers or other third parties.

Transcript

1. **Can you share a few words about yourself and your expertise within the blockchain and NFT field?**

    - **C**: I'm a mechanical engineer, finished my degree last year. I have switched to doing crypto professionally for the last 10 years, as I previously bought bitcoin and sold. Well, when it became more mainstream I bought into it again. Still I didn't understand the purpose before. When COVID hit in 2020 I re-entered the market because the market crashed. However, why blockchain? I see it as Dotcom era would repeat back in the 90s. It's kind of the same situation. What to do with it? Tech is important, but there is not really an application for it.

      With NFTs I've only been very involved in the last 9 months. It's another situation where there's a great idea but a hard way to apply it to everyday life and what we can do with that. It boils down to proof of ownership - having somebody to prove. Where you have these counterfeit pieces - the benefit is that they're unable to prove that it's the original piece. Blockchain will say if it is beneficial or if it's not. Besides this, it's also how does the government get involved?

- **A**: I'm currently in computer science and I obtained a finance degree a long time ago. I've been in startups ever since. I've worked for both companies that made it and that failed. I've mostly been a CTO so far, mostly been in products. I started an NFT company in 2018, tried to do a kickstarter and failed miserably because no one cared about NFTs by that time.

  Now NFTs are suddenly back on the map. I've created a few collections that also failed. I consult NFT projects, I'm advising other projects as well.

  I've been an NFT collector from 3-4 years ago, I have written several smart contracts deployed to the chain for NFTs specifically. I've worked with some of the more interesting ones like ArtBlocks (I also know the founder). Then I've built a crypto wallet in the past, infrastructure, now I'm building another one for another company. In terms of tech stack I'd say I have a deep understanding of how the technology works.

2. **Can the NFT field enable a wider adoption rate of blockchain technology in general? How would this be achieved?**

   - **C**: I would say that there's more of a visual attractiveness towards NFTs rather than traditional crypto, because people can see something. This might get people more interested. The technology itself can be confusing, people might see a blockchain NFT game but they don't know that - they just see the fun stuff happening. That's a grey way to attract people. As an example, in order to play the game if you have to buy an NFT that's thousands of USD then people don't wanna get into it. Therefore, things have to be more accessible, people see this thing and they wanna be a part of it but they don't know how to send the money on a wallet, or to create a wallet, to understand what that is even doing. All in all, accessibility is a huge barrier even if the NFT realm is a great place to attract people. It is still in its infancy.

3. **Where is the blockchain and crypto ecosystem currently situated, in regards to NFT adoption?**

   - **C**: That's a good question. Well, finding use cases is the hardest part - when it boils down to it, what is the point of an NFT? I think one interesting take that's happening now is real estate - someone buying a home and have an NFT certificate to tell somebody else who owns that home. You don't need a real estate agency as a middle man, you can sell something direct to a person without somebody else taking a cut; buyer straight from the seller. The problem is that everyone has to agree that the NFT is a valid resource to show who owns the house. At a higher level of authority - has to agree that the ownership is true.

- **A**: Everything is happening on Ethereum, there are some alternative blockchains that are coming up. If you look at OpenSea being one of the top marketplaces, about 10-15% of the volume of transactions on Ethereum and they often outstrip even DeFi contracts. Overall blockchain is still in their early days, as the reality is that 95% of people still don't interact with it. I see NFT as the bridge, that people are gonna engage with things that are meaningful, collections, that kind of stuff. I think it's gonna accelerate people's onboarding within crypto, if they'll be successful at all.

4. **What is currently missing from the NFT industry and how could these gaps be filled?**

   - **C**: There's a lot of promises and expectations but we're so far away from those promises being fulfilled. My perception is that this trendy word, Metaverse - it's this online video game where everyone in the world can log on and live in this virtual reality. The suits they can put on they can feel touch everything in this virtual world. NFTs have a good benefit for a virtual reality like that - you can sell, buy, trade those digital items in the digital world and I think that's the idea of what's happening right now.

     However, we're so far away from that point. Maybe closer than we think, but not next year. The market is though so heated and there's so much money flowing into this market. People are gonna realise that their expectations are based in reality. The other side of that is that we don't need to have a virtual world - eg. Call of Duty where you can buy specific skins, etc. Even the major gaming companies don't wanna adopt that because where are they gonna get their cut? They are afraid of being left out. To put it in simple words, figuring out for a way for everyone to benefit is still being figured out. There's not a bridge that everyone agrees with so far.

   - **A**: The golden problem that everyone looks at is the experience of actually buying and owning an NFT is really difficult. It's a trade off, it's decentralised and a lot of people give up because of that. Education is missing and that could be new technology that makes that easier. If you look at fraud, people don't understand that they could buy a stolen asset. Assets will get seized and they'll end up without money and their bought NFTs. It's also difficult to seize assets because they're not physical. For example galleries are regulated, auction houses are very regulated in terms of money laundering and KYC. I think fraud stuff is a big thing that's missing.

5. **NFTs are by nature unique, due to the cryptography standards that they embed. However, we have seen several cases of counterfeit NFTs being traded on different platforms, and this is because files are easily accessible even before they are purchased. In these terms, how can an NFT investor verify the authenticity of an asset before purchasing it?**

– **C**: There's a few ways I go about it - it's getting more vague even now because of several things. A lot of these projects have social media accounts - Twitter, Discord. Also there's the project launched, you can look at the contract in Etherscan, you can see how much of the website is built, etc. My typical go to is that if I know that there's huge following on Twitter and people make all their announcements.

  However, still there's verified fake Twitter accounts sending links. That methodology of saying their twitter accounts have 60k followers it's hard to do. I've been reluctant to buy new projects in the last few months because of that. I don't have the risk tolerance to get anything new right now. If I check for verified OpenSea accounts that have their own verified blue sticker on their accounts. The problem is that there are so many different unique ideas and making projects that look exactly the same. Basically, it boils down to looking at the contract on Etherscan - if money is only flowing in it's a red flag - if both ways there's people trading, people buying and selling and that's good. Personally, I'm sticking to projects that have been around for the last at least 6 months. That's a huge red flag for the market because people are gonna stop, the money's gonna stop flowing in and people are gonna sell everything off and the market may tank. It's a forever changing tactic to verify these things.

  I would conclude by telling that some ideas are find the correct community to get valid information, verify where the money is flowing: in and out and check their social accounts, are they fake or legit?

– **A**: This is very philosophical, so it really depends on the NFT. If you have on-chain art where the art is on the blockchain, the NFT is on the smart contract, you have to check that you interact with the actual contract that you expect. If a letter from the address is different you give someone else the money. The real way is to write go to the chain yourself, write the code yourself to understand that, but it's very difficult.

  For the vast majority of NFTs, the story is weird, because a lot of people don't realise is the thing that they're purchasing is actually indexed to an array that is a URL and then that URL goes off to somewhere else and it's often not even decentralised itself. A lot of people also don't understand that URL can be changed by the contract creator so there's actually no guarantees that what you're buying is not the image that you're seeing. They don't understand that the image is on someone's computer and it has nothing to do with blockchain.

  There's just a social agreement, for example, all of the assets from the Bored Ape Yacht Club, you can copy paste those images and sell them on another contract, that's actually not fraud, because they released the rights to it, and that's perfectly legal. So overall it's complicated, it depends on the smart contract.

6. **How should the problem of counterfeiting be solved in this industry?**

   – **C**: That's a good question that needs to be answered sooner rather than later. Especially with these Twitter account scams they need to stop people allowing getting verified accounts for no reason. One area is figuring out how can these companies have verified accounts and people trust them. The marketplaces should have a process to have legitimate projects on their accounts. For example, having 10 different profiles on the same project showing on the same marketplace is a red flag - the process to verify this takes a long time, especially when the market is so heated. There are a lot of money coming in, but unfortunately not a lot of support to be able to verify and put in the correct processes to make sure the scams are showing up. Therefore, it's too much in its infancy phase to try to stop that.

   – **A**: I think the industry is going the other way, like you're seeing with releasing the copyrights, they let it go with this problem. One way is that you don't make it illegal in any collection to counterfeit, because it's a part of it. You can't counterfeit the actual NFT on-chain without attacking the blockchain. You can't take over my NFT or my wallet, it's a smart contract. The type of counterfeiting that exists is someone lying to you that this smart contract is actually the real one and this one not.

     The community would say there's no such thing as counterfeit, they're just smart contracts and if you interact with the wrong smart contract then it's your fault. How do you prevent someone from doing that is really complicated. For example Cryptopunks vs Cryptopunks v1, the original creator tried to retain copyright, and today they sue people for duplicating the collection and reselling it.

     But they also did an interesting thing when they fought with their own contract back in the day, because of a bug. There are 2 Cryptopunks contracts and they say the second is the real one because the first one had a bug in it. Some people started buying and selling the original contract, because they assumed that the second one was just crap, the first one was the real one. So they were trying to take down the original contract, yet the same guys created it. Now it's no longer counterfeit because they said you can do whatever you want with your image, there's no artist copyright in that and that's becoming a strong trend. With the blockchain it's impossible to say that something is actually stolen because the agreements are so loose and they are stored in the smart contract somewhere.

     Marketplaces are doing a relatively decent job at flagging things and saying that for example these collections are no the real ones. But beyond that, it's still a decentralised wild west, but in my perspective, they're not counterfeit. It's literally someone creating another smart contract and I can go by that.

7. **How can we prevent cyber theft and avoid cases as it happened before with platforms like OpenSea where NFTs were stolen from users' wallets with a phishing attack?**

   – **C**: This a tough topic. It boils down to the user. The way everything is set up, the person has to sign these contracts with their wallet, they have to click some approvals in their wallets. People clicked on an email that took them to a really similar website to OpenSea and they approved the scammer. It really gives me PTSD because I don't touch anything - if I don't need to be online I stay offline. I would say that people rush to do things.

   – **A**: One way is building stronger wallets so you can have a registry on-chain, known safe contracts. Like a public good where the community registers legitimate contracts, you're leaning on the community to vote on contracts. You have to have a social consensus because mathematically you can't prevent it. Also encourage users to use restrictive wallets.

8. **Should NFT marketplaces be liable for the content they host? How could they do that if the files are stored on decentralised networks such as IPFS?**

   – **C**: I think yes, they should be liable, maybe not held accountable but they should have a better process of showing authentic projects. For this movement to catch mainstream adoption people need to trust these applications. In order to trust these applications these things need to have a better process of showing legitimate projects. That process itself is still very vague and so in its infancy. How do we provide only legitimate projects? That's gonna be a lot easier when the market isn't so heated.

     There's too many things coming out now and it's hard to keep up. When you have decentralised networks in nature that's where the point is to. It allows people to make these things on their own will. It's necessary to survive long term, but right now it's hard to wrap some process around that whole thing, especially for centralised exchanges.

   – **A**: It depends. If you're taking royalties and you facilitate purchasing not directly on-chain or through code that you've written that goes through a centralised server then I think you are liable, because you are providing tooling on top of a smart contract. If you're a fully decentralised marketplace, I'm not sure if you're liable because technically you're not running any of the code that someone is interacting with. Any images that you're hosting, yeah, you have to follow the laws of your country but it shouldn't suppress any collection.

9. **There are some signs that regulation is slowly coming in place for NFTs, in certain jurisdictions. Should NFTs be regulated and if so, which aspects should such regulation refer to?**

   - **C**: This is a great question. I think it's such a broad and vague area for a lot of people, especially government entities and myself included. It's a vague area figuring out and adding a regulatory process.

     How are you going to track everything? Luckily it's blockchain so you can track. At the same time, people work together, anonymity can be traced. If it's a pool of money coming into a project and dispersed to a lot of people it's hard to follow that. How are people gonna regulate what is a legitimate NFT? Are we gonna allow houses or artwork to be NFTs? Who gets their cut? Governments will also need their cut on it. It should protect innocent people falling for these scams, that's always what they tell you but they just want their cut.

     It's a very touchy thought. From my perspective, I don't want government hands in everything that I do, but I want to make sure that I'm safe. A lot of it is gonna be on the users' side so they can protect themselves. But how are we gonna educate people on that? It should be a huge movement, it should be the next thing for mass adoption. People need to understand what this is. Myself included, I need to continue learning.

   - **A**: I think they should be regulated as property - if I have a painting on my wall and the US government thinks there's an asset, I would have to comply and argue my case. But they have to get a warrant, to have reasonable proof to take that thing off my wall, they have to disclose it to me.

     With NFTs it should be the arguably the same. Regulating the buying and selling of them, I think it's gonna work like property, as marketplaces that will have licenses to do these things. For example I can buy a car from the black market, and maybe somebody registered it as stolen.

     The government will likely have a registry of known smart contracts or NFTs that are marked as illegal and you take the risk if you buy and sell that one. For me, my wallet is easy to identify through the US government so I'd be very cautious interacting with that, I don't wanna know if there's an NFT that was marked as doing money laundering.

10. **Do you see blockchain in itself as a technology that can help in reducing counterfeiting on NFT assets or should it be joined by others (AI, Machine Learning, etc.)?**

    - **C**: You can't counterfeit what is the true contract. If you understand how to verify these things, that should be the idea that it cannot be counterfeit. The problem is that in the NFT realm you don't see the contract, you see an image. Therefore, if the image looks the same, a lot of people think it is the same and that is the issue, a lot of people are blinded on the frontend rather than going on the backend of what is the truth. If there's a better way to authenticate into the blockchain backend I would be able to have a much better vetting process than checking the social media or seeing where the money is flowing.

It's about how do we put that in front of the user - what to look at first? It's gonna be an interesting way to show that. Everything is there if the user wants to see. I didn't understand any of that 8 months ago, or the metadata before. A lot was very vague but it is available to see.

- **A**: If you have a blockchain that has the ability for a third party to change history or approve or deny something, it's fundamentally not a blockchain at that point. No one in the world can access my wallet because I'm the only one who has the seed phrase and that's the fundamental tenet of Ethereum.

  I wouldn't use a blockchain where some party can restrict what I can do because I think that's no longer a blockchain. Even if it's AI, that's maybe not decentralised anymore. I choose to interact with this new contract with this marketplace contract that has AI counterfeiting prevention built in, but that's just a centralised system. We do that in the real world, it's replicating capabilities. They are useful in the digital world, now we can have that freedom.

11. **How can we keep a balance between user privacy and information about the authenticity of the listed assets? Can blockchain assist with this?**

    - **C**: It's completely up to the user. This Web3 idea is that you have a second identity in the digital world. If somebody wants to connect the dots they probably could. If they see the contract of Bored Apes they can follow the address of the original, and trace down to a Coinbase wallet maybe.

      However, I'm not 100% an expert, it's just from experience. But blockchain could definitely protect people that use the technology and that's extremely important. At the same time it's an easy way to identify people. To pick somebody with a wallet - that's traceable forever. They will be able to paint that what comes and goes forever.

      What are willing to do at that point? How does blockchain protect that? It's already anonymous, identity-less so to speak. It boils down if the user puts that information there. I think that definitely there should be help and more clarification for new people joining what they're doing.

    - **A**: It kind of exists, if you have a wallet and create a smart contract, that wallet is the authentic wallet. If that artist wants to create something more, you already know it's the same person, because you can see the provenance of the asset.

The other ways you could have a loose third party like an on-chain registry, a dApp that interacts with the said artist. Banksy is a great example, he has a foundation that validates the Banksy paintings. They act as an intermediary so you can send them a painting from Banksy and they can confirm because they know Banksy. Because you'll never gonna know who Banksy is. An anonymous creator could choose to expose themselves to a trusted third party. So you can ask that third party if the smart contract is the real one.

12. **Do you have any closing thoughts on the topic?**

    – **C**: I've been in crypto for several years. NFT area in the last 9 months has been the most fun and interactive form of crypto for me. It's very interactive because you have these trading cards and you can talk to other people about it. It's a community, it's like this very strong sense of belonging. It's a huge desire for people in general, people want to belong. In this world, anyone can belong.

    It doesn't matter it's a valuable product or not, I've seen lots of projects that are not valuable but there are people that love it, and talk and learn how to mint, design and draw. There is a huge network where people are learning different things about themselves. That's almost priceless depending on where you go. That's my overall thought of NFTs in general, I met lots of interesting people and I enjoy it.

    – **A**: I think I would encourage you to look at on-chain art, maybe ArtBlocks. There's two large categories of art. On-chain is where images are generated by code that lives on a blockchain. So you don't have a hosted image somewhere, but you arguably buy the code itself and you can see a representation of this. SmartBlocks does that and they publish that code in the chain, in the same contract you own the NFT and the source code for it.

    They sell them with 200-300 ETH per piece. If you look at the token URI which is where the metadata comes from, it just returns a bunch of dots and slashes, because the artwork itself is that string of text, there's no JSON or metadata. Those are interesting, because there's just the smart contract, nothing else, nothing to copy. An interpretation of the code. On-chain solves a lot of these problems because it's self contained.

    Also I was working with an artist that wanted to have their mints into a smart contract that had copyright protection built into that. They were publishing the legal language in the smart contract itself, which is kind of interesting, like the on-chain. There are some projects on that matter.

A.2 | User Survey

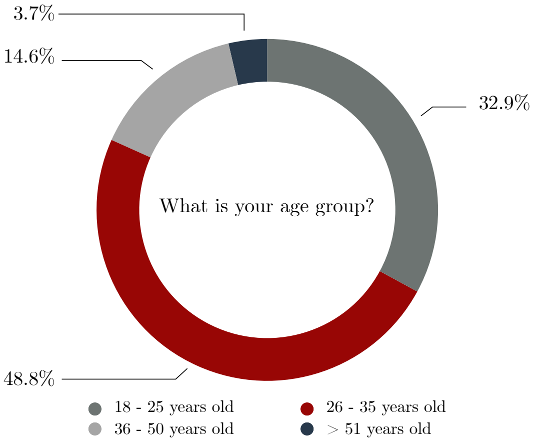


Figure A.1: Survey Question 1

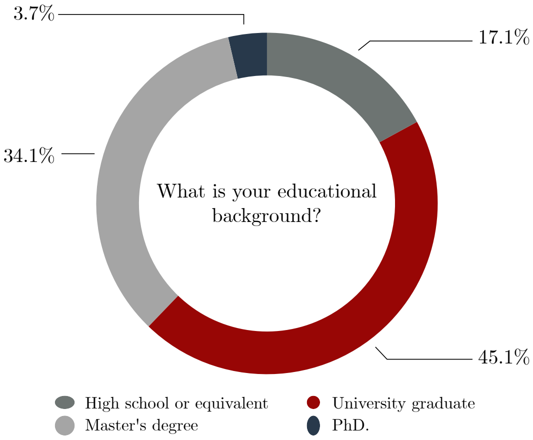


Figure A.2: Survey Question 2

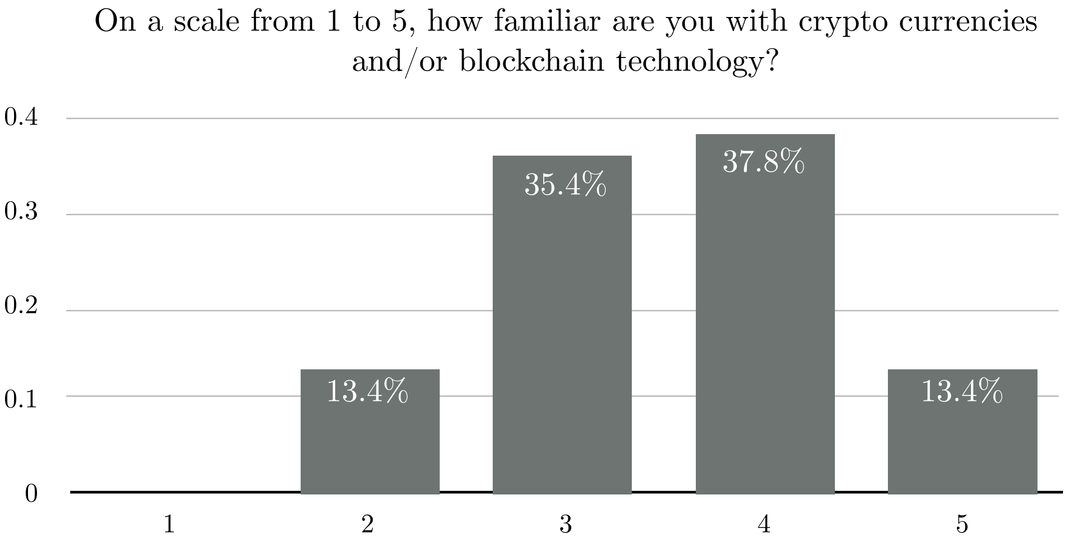


Figure A.3: Survey Question 3

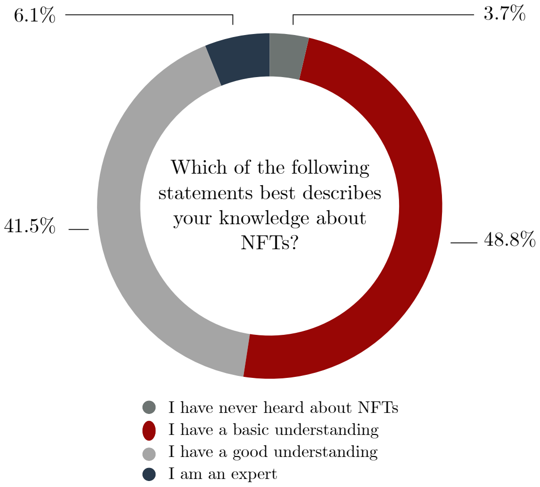


Figure A.4: Survey Question 4

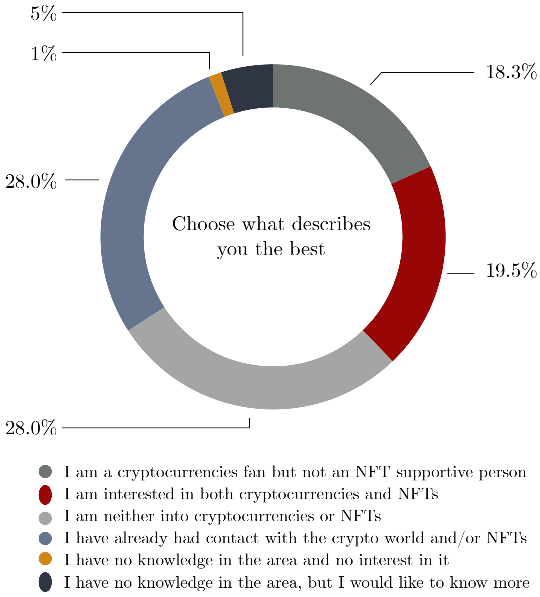


Figure A.5: Survey Question 5

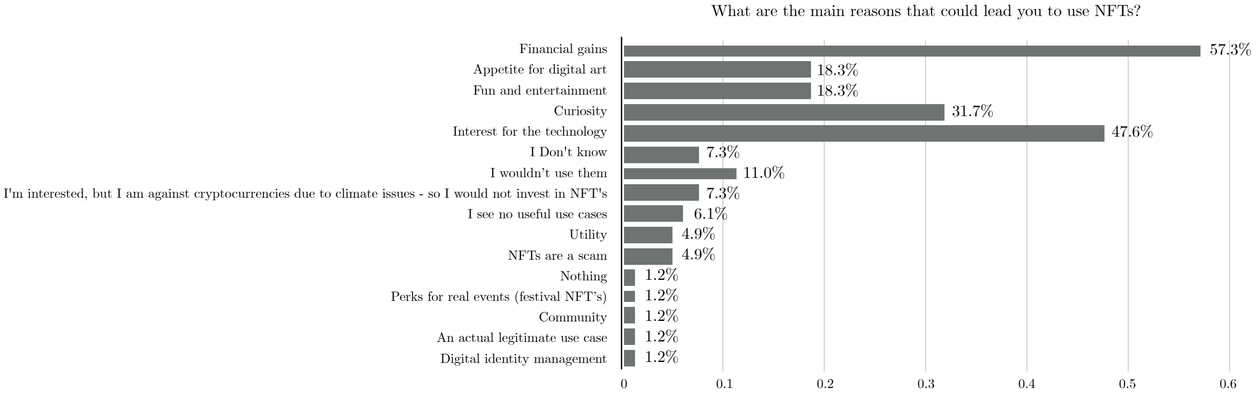


Figure A.6: Survey Question 6

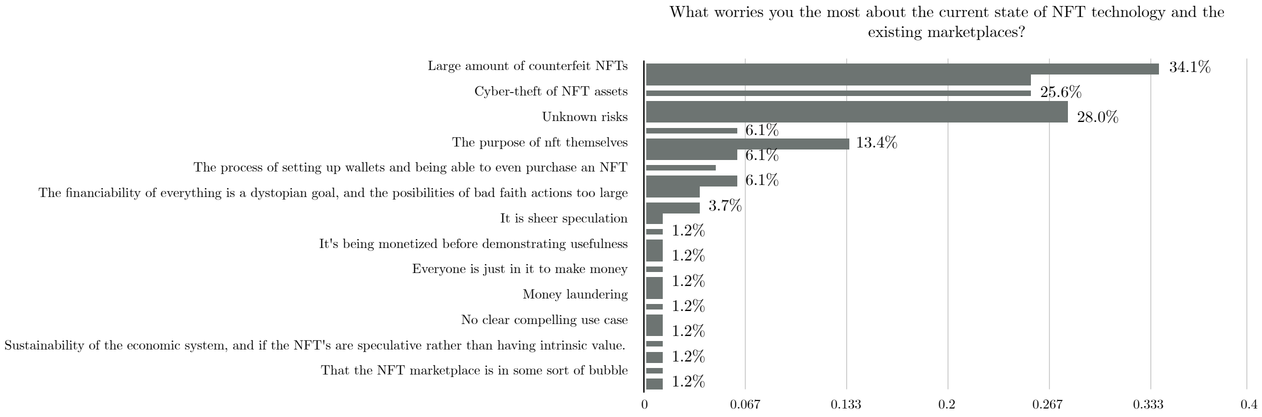


Figure A.7: Survey Question 7

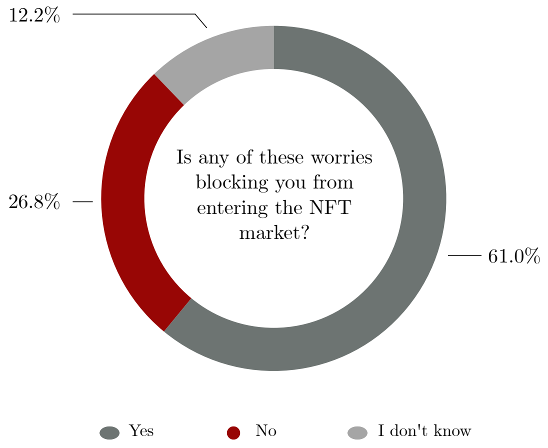


Figure A.8: Survey Question 8

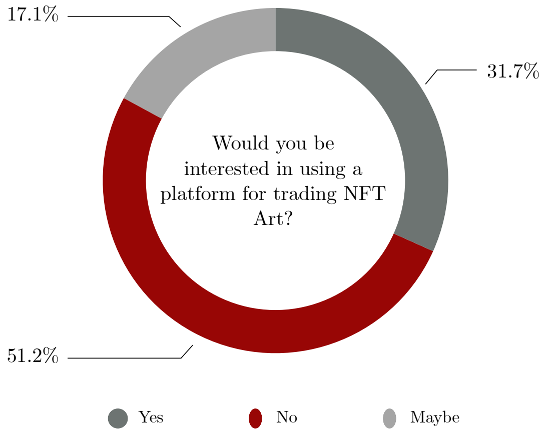


Figure A.9: Survey Question 9

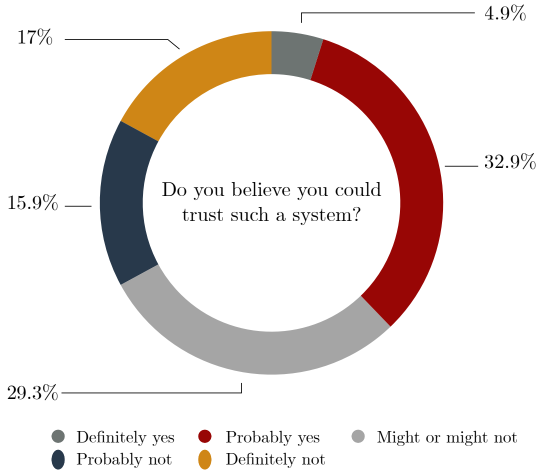


Figure A.10: Survey Question 10

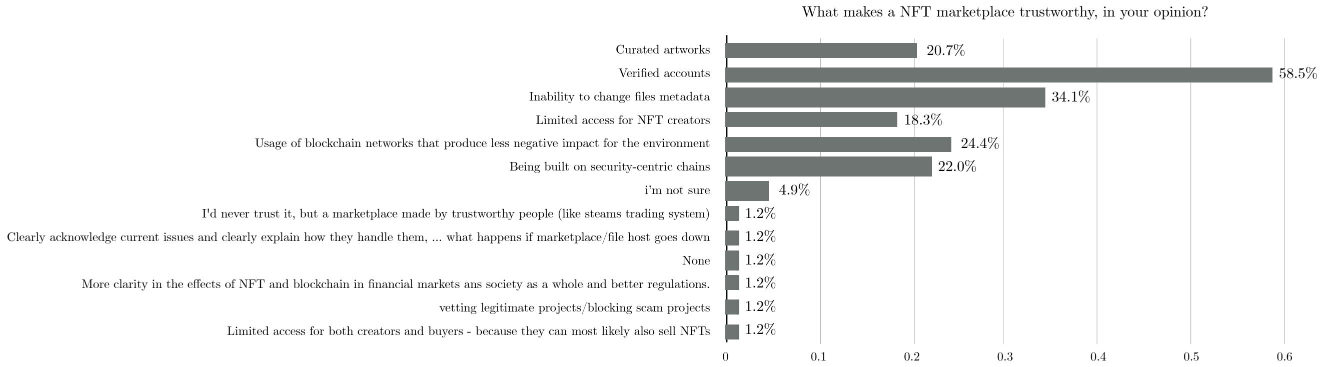


Figure A.11: Survey Question 11

Do you have any other suggestions?

- Such NFT marketplaces have already emerged, but there's still a lot of problems with counterfeiting and other security problems. In it's current form a lot of responsibility rests on the user's shoulders to properly vet projects before buying into them. Crypto is about everyone having the ability to take ownership of the system/service and therefore it's hard to create such a system without excluding people and having the infrastructure built in a way that doesn't require some level of trust between users.

- I've been thinking about NFT's in a very financial way. Basically thinking of it as a way for digital artists to make money, but also for buyers to buy(for personal use) and/or speculate on investing simply to make a profit

- Generally artwork NFTs are not particularly interesting to me - despite being invested in a few crypto projects. I think the fact that digital art can be recreated many times over without losing quality is a net positive, because it allows more people to enjoy the art (non-commercially), facilitate network effects for the artist that can then be used to turn a profit etc.. I'm not a huge fan of artificially trying to limit that - besides there's already copy right protections etc. in place. With 'real art' the original has some qualities that can't easily be replicated 1:1. With game-skins digital art has some intrinsic value as it can be argued that it adds to the gaming experience. In my humble and somewhat uneducated opinion, artwork NFTS need to improve something, add to something, have better quality then counter-parts etc. Simply being able to say something along the lines of ”I verifiably own the first copy of this file” has little value to me. But then again - I'm no collector. GL with the thesis :)

- Easy guides to understand how to enter the market as a buyer/seller.. basically a super easy and understandable manual

- I see no problems nft markets solve in a useful way

- Money laundering concerns

- Regulate the hell out of digital currencies, blockchain and any online ”opportunity” that has to aggressively recruit new victims - see NFTs. Regulate the hell out of those that market itself to vulnerable populations and their in-crowd to get fresh blood in and keep victims from liquidating their 'assets' by promising large returns on an inherent valueless 'product'. Or even better: Shut that whole experiment down and sue everyone profiting from it. I'm tired, and I hate that this has to exist and I have to report 10 ads a day on whatever platform because they are promising me ”-insert large amount of money here- by this time tomorrow” if I join their crypto or NFT scheme.

- I think that a big barrier to NFTs is digital literacy (knowledge of the cyber space, and access to easily acquired knowledge about blockchain and NFTs and their function in society). Most people who gain an understanding are young, digital natives who might already be involved in digital or IT communities.

- people don't purchase art, how many friends do you have which display art on their walls. people purchase brands, status, symbols - branded NFTs should be a thing imo
- IMHO, NFT is currently basically a scam. Perhaps things will be different in 10 years.
- I have worked both in ”traditional” finance (mortgage lending) and in fintech. I love cryptocurrency and invest in it, but I am apprehensive to invest more in it along with NFT's, mainly because I am not fully sure if the value of NFT's is purely speculative or if it has intrinsic value. I am still a fan of traditional investment methods such as real estate investing, as there is an actual product that retains value.
- Security and rug pulls need to be addressed. The creators need to be doxxed.
- The user interface on some of the NFT platforms are hard to navigate.
- Explore NFT on all of the blockchains - ETH is getting too expensive to use
- In order to increase the trustworthiness of marketplaces there needs to be more regulation and transparency with the marketplace.
- It is not trustworthy to me and never will be in any form. And it saddens me greatly to see that people are finding even more stupid uses for blockchains which are harmful to our already suffering planet.
- Cryptocurrencies do not cause climate issues. For example, not a single BTC miner produces CO2. The mining machines usually connect to an existing grid. Also, Miners can reduce their load on the grid per request basically immediately if requested, whereas nothing else on a grid can do that. This way they can serve as a stability point of a grid in extreme times.
- It is not so much about NFTs for me, but cryptocurrencies in general: How easy it is for content creators to pump-and-dump scam their audiences. Also, NFTs incentivise more crypto currency mining, and thus more energy wasted due to proof-of-work

B User Testing

Purpose

The purpose of the user and usability testing process was to validate the `Smart NFT` solution desirability and to obtain feedback that would be the basis of the future improvements that should be implemented.

Respondents and Testing Methodology

Five respondents from the author's network have been selected, all of them having at least a basic understanding or minimal contact with the blockchain or cryptocurrencies field.

Used methodology: remote user/usability testing with the Think-aloud protocol.

Used tools: Google Meet for video communication, TeamViewer for remote access, `Smart NFT` app running on a Hardhat local blockchain instance.

Evaluation Technique

The evaluation process consisted of qualitative data, as keeping a record of the most relevant notes and thoughts from the users, and quantitative data, as assigning a complexity score to each task, in the range between 1 to 5 (1 being 'effortless' and 5 'highly demanding'), depending on how easily did users accomplish the task. The scores are documented with histograms and the obtained means.

User Tasks and Test Results

1. You have just connected your crypto wallet to the `Smart NFT` platform, which is an NFT marketplace accessible only to verified users. Browse through the marketplace and navigate to the user profile of the creator of your favourite NFT listing.

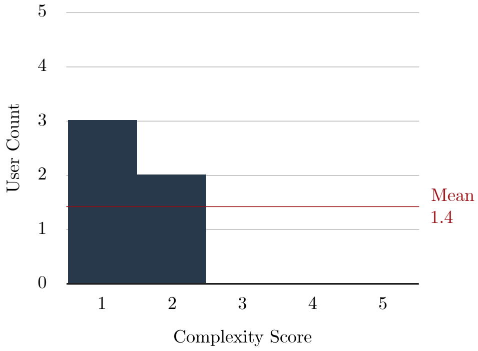


Figure B.1: User Task 1 | Complexity Score

Relevant observations

- Respondent 2: 'OK, first I'll get to the marketplace, I think I'll use the nice sidebar icon... The one with the zebra looks great, I see that there's an artist address so I think that's where I should click. Oh, here it is!'
- Respondent 3: '... quite a few nice ones, I'll pick this. Oh this took me to the NFT page I guess... Here it was, artist.'

2. As you might have noticed, you can navigate all over the platform, but you cannot perform any transactions until being a verified user. Find and submit the verification request form that will subsequently be approved by an admin user (you can and should use dummy data).

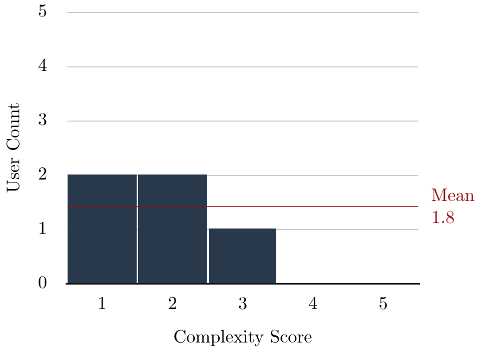


Figure B.2: User Task 2 | Complexity Score

Relevant observations

- Respondent 1: 'Yeah, noticed I can't buy any items because of that. Don't get me wrong, it's a great idea to verify users, but should I trust this with my real data?'
- Respondent 3: '... I got the 3 images, clicked on Submit but now this Metamask thing popped up. Didn't know I have to pay for this, good that its test ETH. And nice, I have a profile now!'
- Respondent 4: '... I'm completing random data... Trading details, isn't that too intrusive? I hope it's stored somewhere securely.'

3. Your verification request has been approved, and you currently have the `verified` status. Find your favourite NFT asset in the marketplace and purchase it with the test ETH in your connected crypto wallet.

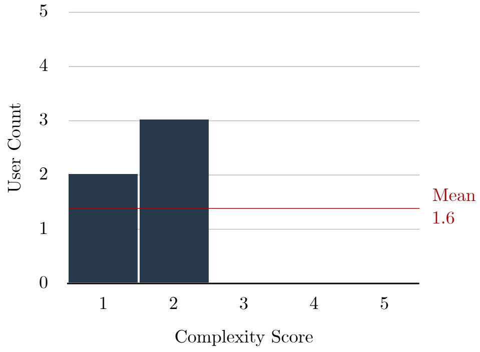


Figure B.3: User Task 3 | Complexity Score

Relevant observations

- Respondent 2: 'Back to marketplace, I can click Buy now. I'll go for the zebra painting again. That was quick, I think it worked, right?'
- Respondent 5: 'That looks straightforward, let's see. I can click, now I approve and... It's done. It almost seemed too fast, what if I made a mistake?'

4. Find and your newly purchased NFT.

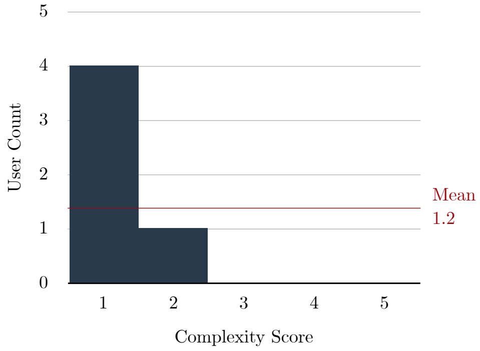


Figure B.4: User Task 4 | Complexity Score

Relevant observations

- Respondent 1: 'Nice, that was easy because I was redirected to my user page, so I just had to click on 'Owned NFTs'.'
- Respondent 4: 'I would look for some dashboard, but I see the 'Owned NFTs' text there, so that's where I'll go.'

5. Let's pretend that you would also like to become an NFT artist. Find the form for uploading a new NFT and listing it to the marketplace (you can use any image from the Internet).

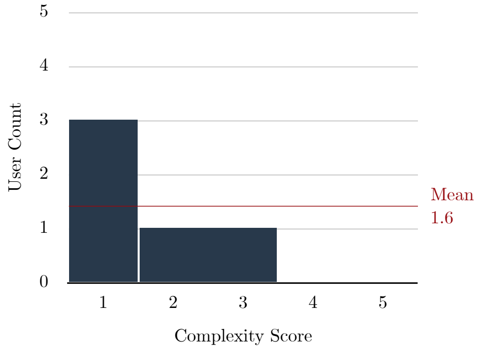


Figure B.5: User Task 5 | Complexity Score

Relevant observations

- Respondent 2: 'I like that the button encourages you to click it. Let's find an image and add the name, price...'
- Respondent 3: '... Nice that I could see the ETH price in dollars in real time, I was just gonna ask for that.'
- Respondent 5: '... and submit. Why did I have to approve twice? Anyways, it worked so that's good.'

C System Installation Guidelines

Prerequisites

- Yarn Package Manager
- Hardhat
- Firefox Browser
- MetaMask Wallet
- Infura Account

Installation Guide

1. In the root directory run `yarn` to install dependencies.
2. Create an account on infura.com and create a new Ethereum project.
3. Go to the project settings page under the Keys tab and select the `POLYGON MUMBAI` endpoint from the dropdown. You will get the `PROJECT ID` and `PROJECT SECRET` keys that you will use in step 5.
4. In the root directory create a new file called `.env.local` to store the environment variables.
5. Add the following content in the newly created file:

   ```
   INFURA_PROJECT_ID=yourProjectId
   INFURA_PRIVATE_KEY=yourProjectSecret
   NEXT_PUBLIC_SECRET_KEY=yourSecretKey
   ```

   where `yourProjectID` is the `PROJECT ID` value from step 3, `yourProjectKey` is the `PROJECT SECRET` from step 3 and `yourSecretKey` is a random string you should pass.

Running the dApp

1. In the root directory run the following command to start a blockchain local instance:

   ```
   yarn run blockchain
   ```

2. Open a new Terminal tab and run the following command in the root directory to compile the smart contracts:

   ```
   yarn run compile
   ```

3. To deploy the contracts to the local chain and to start the dApp run the following command in the root directory:

   ```
   yarn run dev
   ```

Using the dApp

1. Make sure that you have the MetaMask browser extension installed in Firefox.
2. Create a new MetaMask wallet by following the steps provided in the extension interface.
3. After creating the wallet, connect the extension to the local Hardhat network that you have running in Terminal window 1 by following the steps in the linked article.
4. Switch to the newly added network, click your avatar and click `Import Account`.
5. Go to the top of the Terminal window where you run the Hardhat blockchain instance and copy the private key associated to Account #0.
6. Paste the private key in MetaMask and press `Import`.
7. You are now ready to connect your wallet to the `Smart NFT` dApp.
8. Re-iterate from step no. 5 to be able to connect a new wallet (i.e. user) but use any of the other private keys.
9. *Bonus step*: Any created user in the KYC step (including admin user) needs to be *Approved* before being able to mint, buy and sell NFTs. To create an Admin user type add a KYC verification request and use an email address of shape `*@smartnft.com` in the form. You can then approve yourself and other pending users.