FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

Distributed Ledger Technologies and NFTs in Healthcare Scenarios

Luís Miguel Almeida Fernandes

U.PORTO

FEUP FACULDADE DE ENGENHARIA UNIVERSIDADE DO PORTO

Mestrado em Engenharia Informática e Computação

Supervisor: Alexandre Valle de Carvalho (FEUP)

Supervisor: Khadija Sabiri (Associação Fraunhofer Portugal)

July 25, 2022

Distributed Ledger Technologies and NFTs in Healthcare Scenarios

Luís Miguel Almeida Fernandes

Mestrado em Engenharia Informática e Computação

July 25, 2022

Abstract

In healthcare, patient data consists of the information regarding all events of a patient towards diagnosis, symptoms, diseases, treatments, or any other medical-related procedure. A patient data record is usually created every time the patient goes to a hospital, health center, or any different kind of medical facility. The way patient data is represented and stored substantially impacts how easy the patient has access or other professionals need to consult the historical record to make further decisions regarding medical care, despite their situation.

Currently, medical information is not only ineffectively stored because it is not entirely available to the patient, everywhere. It may also lack records of events, or it is often duplicated across multiple systems. Furthermore, a patient cannot grant access to their medical records to other healthcare professionals and cannot ensure the privacy of their data.

Current work reviews go over the state-of-the-art techniques for DLT and NFT and their possible utility in the medical field. The possibility of assigning each patient with personal NFTs where information will be uploaded every time that patient has any appointment or medical procedure will be explored in the prototype, testing the evolution of this system over time and its possible viability. With the data collected and after analyzing it, the prototype was assessed to be, or not, a good fit for this scenario.

To assess viability of these technologies, a prototype was built where one could upload files as NFTs with extra appended data which would be encrypted and could later be accessed and decrypted by providing the application with the corresponding keys. All NFTs would be present in the patient's personal wallet and could not be accessed in any other way. This prototype was developed as a proof of concept, in order to find out if the approach is possible, and is not intended to produce quantitative results comparable to currently existing approaches.

The results show that the concept is in fact valid and that the technologies surrounding NFTs can be used as a helpful and viable option for storage of valuable information such as a personal medical history. It is viable in the sense that it can keep important files for someone and later be checked by the owner of that information and shared by the patient accordingly when necessary. This concept is however still new and needing to mature in areas such as the legislation surrounding medical information and how healthcare facilities can interact with it, but if further explored, can be a helpful approach to the problem at hand.

Keywords: Blockchain, NFT, Patient Information, Healthcare

Resumo

Nos cuidados de saúde, os dados do paciente consistem na informação relativa a todos os eventos de um paciente para o diagnóstico, sintomas, doenças, tratamentos, ou qualquer outro procedimento relacionado com a medicina. Um registo de dados do paciente é geralmente criado sempre que o paciente se desloca a um hospital, centro de saúde, ou qualquer outro tipo de instalação médica diferente. A forma como os dados do paciente são representados e armazenados tem um impacto substancial na facilidade de acesso do paciente ou na necessidade de outros profissionais consultarem o registo histórico para tomarem outras decisões relativas a cuidados médicos, apesar da sua situação.

Actualmente, a informação médica não é apenas armazenada de forma ineficaz, mas também não se encontra inteiramente disponível para o paciente, em todo o lado. Pode também carecer de registos de eventos, ou é frequentemente duplicada por múltiplos sistemas. Além disso, um paciente não pode conceder acesso aos seus registos médicos a outros profissionais de saúde e não pode assegurar a privacidade dos seus dados.

As revisões de trabalho actuais analisam o estado da arte das técnicas DLT e NFT e a sua possível utilidade no campo médico. A possibilidade de atribuir a cada paciente com NFT pessoal, onde a informação será adicionada sempre que o paciente tiver qualquer consulta ou procedimento médico será explorada no protótipo, testando a evolução deste sistema ao longo do tempo e a sua possível viabilidade. Com os dados recolhidos e após a sua análise, o protótipo foi avaliado para ser, ou não, um bom ajuste para este cenário.

Para avaliar a viabilidade destas tecnologias, foi construído um protótipo onde se podia carregar ficheiros como NFT com dados adicionais anexados que seriam encriptados e poderiam mais tarde ser acedidos e desencriptados, se fornecidas à aplicação as chaves correspondentes. Todos as NFT estariam presentes na carteira pessoal do paciente e não poderiam ser acedidas de qualquer outra forma. Este protótipo foi desenvolvido como uma prova de conceito, de forma a averiguar se a abordagem é possível, não tendo como objetivo a produção de resultados quantitativos comparáveis às abordagens atualmente existentes.

Os resultados mostram que o conceito é de facto válido e que as tecnologias que envolvem as NFT podem ser utilizadas como uma opção útil e viável para o armazenamento de informações valiosas, tais como um historial médico pessoal. É viável no sentido de que pode manter ficheiros importantes para alguém e mais tarde ser verificada pelo proprietário dessa informação e partilhada pelo paciente em conformidade, quando necessário. Este conceito é, contudo, ainda novo e precisa de amadurecer em áreas como a legislação em torno da informação médica e a forma como os estabelecimentos de saúde podem interagir com ela, mas se for mais explorado, pode ser uma abordagem útil para o problema em questão.

Agradecimentos

As none of this would be possible on my own, i would like to take this chance to thank everyone who made this journey possible and who helped me finish this chapter of my life.

First of all, none of this would be possible without the help of my family, especially my parents who provided me with everything i needed to conquer this goal in my life, and gave me amazing emotional support whenever life seemed hard.

Secondly, my supervisors, Alexandre Valle de Carvalho and Khadija Sabiri who guided me to the right path and provided me with feedback and support during this study.

Lastly, i would like to thank my amazing friends and all of the people i met along the way during this stage of life, as they all, in one way or the other, impacted my path.

Luís Fernandes

“There are two rules for success:
1. Never tell everything you know.”

Roger H. Lincoln

Contents

List of Figures

Chapter 1

Introduction

This introductory chapter will explain the context of the dissertation, what motivated this theme, what approach will be used when researching this theme and the expected results of the experiment. The chapter is divided into 5 sections. Section 1.1 will introduce the context of the project at hand. Section 1.2 focuses on the motivation behind this topic and the work that will be developed. Section 1.3 is the hypothesis around which the dissertation will be developed. The chosen approach to the topic presented in Section 1.2 and the expected results are explained in Section 1.4. Last but not least, Section 1.5 contains the structure of the document.

1.1 Context

Every time we attend a medical care facility, we share personal information with that entity, and after the appointment, exam, or surgery, that same facility keeps the records resultant from the care that was provided by them to us. Most medical facilities have their own medical database, containing all of these records for patients that have used their services, but this database is, in most cases, a local database. This means that all of the information retrieved and generated by that facility is primarily available only to people from the same entity, a healthcare center, a hospital, or even a chain of medical facilities.

Many options have arisen over the years to change and try to improve the way patients' medical data is stored in these facilities, one of them is the use of DLT as decentralized storage of information and NFT's, which are stored in a DLT and can append various pieces of information into a token. This approach is, however, recent and still being explored as being a viable replacement for the way information is currently stored and, although there are still no certainties that it will significantly improve the now existing system, there are quite a few already running applications and scenarios which may prove to be helpful in the near future.

1.2 Motivation

The problem at hand can be split into three different issues. The efficiency of the storage of information, the security, safety, and availability of our patient information, and the decentralization of this information, can allow the shift in control of information from individual entities into the person whose data belongs to. After an analysis of the medical records of healthcare facilities, it was pointed out that documents were being poorly stored, being unnecessarily duplicated, or even having lost some previously performed medical procedures.

The security, safety, and availability of the patient information related to the fact that even though current data storage systems are reliable and robust, depending on a single point may present itself to be a liability, meaning that compromising one entity is enough to break the trust of the users or even to allow malicious activity. Being centralized means that the information is focused, allowing for a single point of failure, which can make the diagnosis process harder than it needs to be. And last but not least the shift in control of the information which comes as a result of a wave of awareness about the dangers of technology nowadays but also of the importance of controlling our own personal and sensitive information, which can be misused without our consent when we're not the ones handling it. Examples of this are medical information being sold to companies without our knowledge and without us preventing it. As it stands, it is believed that there is a way to solve all of these problems with the use of some of the technologies that have been surfacing and showing promise in various fields.

1.3 Hypothesis

Within the scope of healthcare, NFT's can be used to keep the patient's sensitive and relevant health information, giving them full proof of ownership over this content and allowing for easy access and full control over who has access to this personal information for how long. Blockchain is associated with NFT's as it will be where the information linked to the NFT is kept in a safe, non-modifiable way to ensure the safety and preservation of these medical records for the future whenever they are needed. This is guaranteed by the fact that the information contained in an NFT is actually stored in a DLT, a decentralized storage, which is cryptographically secure, is immutable, meaning it can't be tampered with. Still, the NFT standards allow for appending multiple blocks of information, which makes it possible to append future obtained information. The token itself would allow for a way for the user to prove ownership over that information and allow access to it when going to healthcare facilities, despite them being the same or different every time.

1.4 Approach and expected results

Given the fact that the topic itself, although having some scenarios is relatively recent and a "new" approach in this field, the starting approach will be to explore the various possibilities of how to implement this scenario given the existing technologies. At first a comparison between the leading existing blockchains which support NFT's will be made. This comparison will consider the terms of the access to the personal information in the blockchain, the data privacy, the transfer of the data's ownership for specific situations such as incapacitated patients. By weighing out the pros and cons that come with each available scenario, we can choose the one which fits this hypothesis the best and by begin implementation if possible. As far as implementation is concerned, the objective would be to create a public platform, which would store the medical information of patients, respecting the currently existing patient information standards and make it available to the patient in question and only that patient, allowing him to carry that information and have proof of ownership over it. With this implemented, the next step would be to allow this information to be shared whenever the user requires medical care at a particular hospital or healthcare facility, allowing them to access the information and use it as best as possible, but then reverting that access to the patient's information when the process is finished. The entity is no longer in use of that personal data

1.5 Document structure

In this document, chapter 2 introduces DLT and NFT, the technologies that we wish to explore in the context of healthcare, discusses their main characteristics, core ideas and some of the work that has already been developed using these concepts, both outside and in the medical industry.

Chapter 3 mentions the problem at hand and the way that we have planned to utilize the technologies in order to prototype a possible solution.

Chapter 4 goes over the implementation of the solution prototype in detail, highlighting the parts of that same prototype and the technologies involved in each step, going in depth on what these were used for and what they bring to this work. This will be followed by chapter 5 which outlines the use case and details the experiment process and the metrics with which the prototype was evaluated.

Chapter 6 concludes by summing up what was achieved, how this compares to the problem that was proposed in the beginning and to the expectations for the prototype, following it up with the points that could be improved upon in this prototype and other areas relevant to explore in order to achieve the best results possible in the future.

Chapter 2

State of the art

The focus of this chapter is to present the state of the art regarding the technologies of Distributed Ledgers and NFT, focusing on their currently existing and other possible applications to the medical field, specifically patient data. Section 2.1 introduces DLT, its types, the way the data is stored, how information is validated and how applications can be build on the DLT.

Secondly, section 2.2 introduces NFT technology, its definition, upsides of this technology and its common use cases as of the current time.

Following 2.1 and 2.2, section 2.3 shows already existing approaches in the medical field with the use of the technologies previously introduced.

Finally, 2.4 helps give some insight on how medical data is processed and stored as of now and what standards should be taken into consideration when trying to approach this topic.

2.1 Distributed Ledger Technology

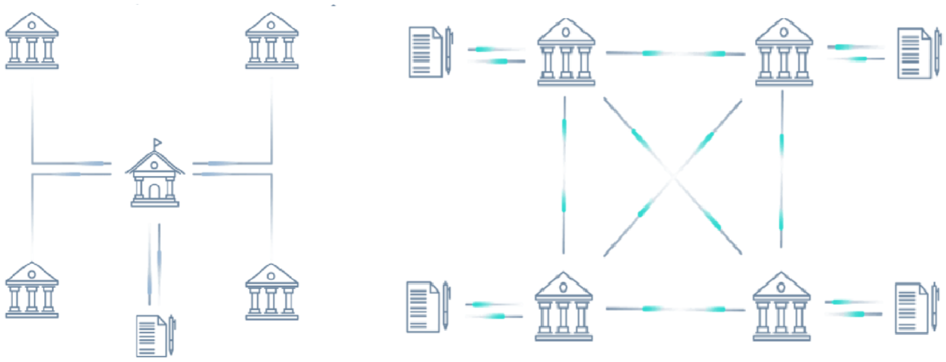


Figure 2.1: Centralized Ledger (On the Left) and Decentralized Ledger (On the right) [6]

Contrary to most current businesses which rely on a centralized database where all the data is stored in a single location, a Distributed Ledger is a decentralized database shared among multiple individuals, called the nodes of the network [35] as shown in figure 2.1. This property allows the prevention of a single point of failure as the same data exists in every node. The fact that a DLT is decentralized also means that there is no central authority or an intermediary responsible for processing, validating and authenticating the network's transactions as the ledger is only updated after the belonging nodes reach an agreement, by the means of a consensus algorithm.

Upon approval, each file is then timestamped and given a distinct cryptographic signature. Since all participants have access to the records in the database, the DLT becomes a verifiable and auditable record with all of the recorded data.

DLT is also a general term, which means there are multiple types of DLT [28]. These will be explored in the following section. Each has its way of storing information, with different advantages and setbacks.

DLT is being explored as a solution to the presented problem since security and privacy are some of the advertised upsides to this type of technology, both relevant in this particular case.

Despite this, DLT also faces some disadvantages, which must be weighed before committing to such technology. They might slow down the whole process and be detrimental to the implementation. Some of these are the scalability difficulty in some cases or even that the ledger is immutable. Immutability might be a great advantage when preventing information forgery, but it also means no one can change any information after it is a part of the ledger [21].

2.1.1 Properties

Security

DLT technologies are used as a means of storing data, some more sensitive than other, but in general, the data should be as secure and private as possible, especially when medical data is concerned, as there is a high probability the information will be of sensitive nature. Because of this, there is the need to make sure that whatever technology is used to store this information can provide such security. The network security is one of the main advantages of this technology and is achieved thanks to the decisions not being made by only one or two nodes, in most Blockchains, transactions must be approved by majority of the existing nodes, meaning that a single malicious node is not enough to approve a "bad block". Depending on the type of network, the information might not even be able available for every node to see. Due to this, the type of network chosen depends on the scenario at hand and can vary from situation to situation. Lastly, the cryptographic algorithms used for the encryption of the blocks aswell as for the generation of keys bring the overall security of the Blockchain to a very high standard [26].

Decentralization

The term decentralization is one of the first that comes to mind when one thinks explicitly of DLT and even Blockchain. Decentralization alludes to the fact that this type of network, made out of multiple peers, shifts the supervision and the decision-making from a single entity. This shift limits the amount of trust that participants must place in one another and prevent them from exerting power or control over one another in ways that harm the network's performance [17].

Although decentralization has its benefits and proves to be beneficial to a network, this decentralization is never total and the closer a network gets to this being fully decentralized, the more struggles it faces due to the data being replicated and spread across multiple places, being possibly easier to access in case a node is compromised, this depending obviously on the transparency of the network, which also depends on the type of network.

Transparency

The transparency of a DLT highly depends on its type and what kind of data is being stored in it. In a public DLT, transparency is higher, and every node of the network can access and view information at any given time. At the same time, a private DLT might impose certain restrictions on what data is available to what nodes. There is a need for a balance between security and transparency, which should be adapted to each use case of this type of network [22]. Transparency makes the ledger fully auditable and valid, which makes it more secure, as everything in the network can be checked at any time. Poor transparency could indicate an attempt at committing fraud, but since everything is displayed and available for any network nodes to check, there is no point in it, as anyone could detect it.

Immutability

Given the nature of a Blockchain, after a block is written and given its cryptographic hash, it can no longer be altered or modified. This can be great as it proves that the network is tamper-proof after the information is validated and written, but at the same time, since no previous block can be altered, data needs to be verified before being approved and submitted into the Blockchain, as one can never come back to correct it [18].

The main danger for Blockchain would be a 51 Percent Attack. In this type of attack, if an attacker acquires very high computing power over the other peers of the network, making him responsible for the next block and allowing him to alter it before writing it into the database, creating a possibility to tamper with transactions for their benefit. This attack, however, becomes more challenging to execute the more peers are in the network [21].

Scalability

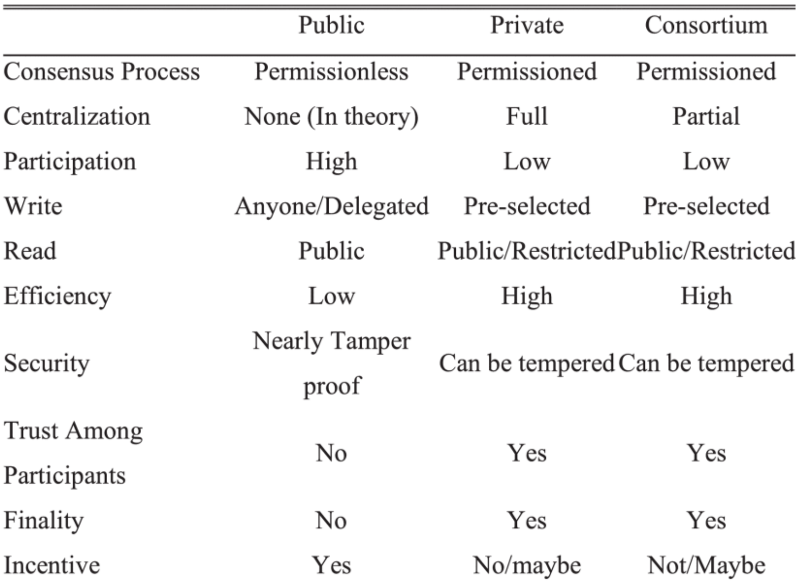
As one of the biggest concerns about DLT, scalability refers to the ability of a network to grow while maintaining a good performance. However, a handful of issues negatively impact a growing Blockchain.

As a Blockchain grows, due to higher demand, there is an increase in the computing power necessary to validate the growing amount of transactions, which eventually leads to higher transactions times and, as a result, higher transaction fees. This increase in the number of validations as people start adopting this technology has also led to the rise in blocksize [23] and the amount of stored information, which poses a setback to the scalability as each node has too much information to store. This is primarily a hardware limitation, but it makes it harder for nodes to keep up with the growth of the network.

Types of Blockchain:

The most common type of Blockchain is known as a **Public** or **Permissionless** ledger. They're designated as Permissionless because the nodes that constitute the network can be anyone and are not controlled. Any entity can become a miner, becoming, in turn, a node of the network as well. In this type of ledger, the information is usually public, accessible to any node of the network. This comes with the downside: all of the data approved and stored into the Blockchain is public and cannot be hidden from any of the nodes contributing to the network. One very known example of this type of Blockchain is Bitcoin [36].

Opposed to **Permissionless**, there are also **Permissioned** ledgers, which, as the name suggests, are controlled by organizations and do not accept anyone to become a node of the network, as usually, these types of Blockchains deal with more sensitive information, most likely belonging to a particular company or a set amount of companies. However, Permissioned ledgers can be separated into two groups depending on the number of entities that act as participants in the network. If there is only one entity responsible for ensuring the Blockchain, it is defined as a **Private** Blockchain. If, however, the Blockchain is controlled by more than one organization, it is called a **Consortium** or **Federated** Blockchain [40] as seen in figure 2.2. In these types of Blockchains, the group of entities controls the consensus mechanism and has predetermined nodes.



	Public	Private	Consortium
Consensus Process	Permissionless	Permissioned	Permissioned
Centralization	None (In theory)	Full	Partial
Participation	High	Low	Low
Write	Anyone/Delegated	Pre-selected	Pre-selected
Read	Public	Public/Restricted	Public/Restricted
Efficiency	Low	High	High
Security	Nearly Tamper proof	Can be tempered	Can be tempered
Trust Among Participants	No	Yes	Yes
Finality	No	Yes	Yes
Incentive	Yes	No/maybe	Not/Maybe

Figure 2.2: Types of Blockchains

2.1.2 Consensus Algorithms

A Consensus Algorithm is one of the main components of a DLT. The main purpose of the algorithm is to decide which one of the nodes of the network will be responsible for writing the next block of transactions and helps protect the network from malicious nodes as it prevents a single node from writing a high amount of blocks. The algorithm is triggered as soon as the network reaches a consensus about the approval of a block of transactions. There are many known consensus algorithms as well as derivations of these depending on the use case [41].

Types of consensus mechanisms:

- **Proof of Work (PoW)** - is an algorithm based on solving a computationally intensive puzzle that requires carrying out resource-intensive computations. A user who can solve this puzzle can publish the next new block in the Blockchain network. This algorithm bases itself on the fact that the high computation and energy costs of writing a block will discourage users from trying to cheat the system [29]. This method doesn't allow use, however to detect and eliminate malicious users.

  > "It makes it expensive to cheat, but profitable to act honestly" [11].

- **Proof of Stake (PoS)** - A common alternative to the PoW consensus is the PoS algorithm [37]. The likelihood that a user will publish a new block in the network is based on the percentage of their stake in the total staked cryptocurrency in the Blockchain network. When they invest in a considerable stake, which is usually an amount of cryptocurrency, the possibility that they will destroy the network diminishes, as damaging the network would, in turn, hurt the staked assets.

- **Proof of Authority (PoA)** - Based on publishing, users' partial trust, which relies on their real identities, must be verified, proved, and included on the Blockchain network. The central idea behind this mechanism is that a publishing user's reputation or identity is staked to publish new blocks [9]. This model relies on a reduced amount of trusted nodes, which increases scalability in the overall system. The increase in difficulty becoming a validator in these networks minimizes the chance of selecting a malicious validator that might hurt the system.

- **Proof of Elapsed Time (PoET)** - An algorithm where each publishing user requests a wait time within the network from a hardware time source secured and installed in the user's computer system [13]. The hardware produces a random wait time for the users, making them become inactive during that wait time. When the publishing user is reactivated, the user creates and publishes a block on the network, and all the users in the inactive state will stop waiting, and the whole process will begin again.

- **Proof of Burn (PoB)** - A mechanism that helps reduce the high energy costs of algorithms like Proof-of-Work. Following the principle of "burning" tokens owned by each miner, granting them the right to mine after being expended. This algorithm aims to stop the double spending of tokens, one of DLT's most dangerous attacks. The burned tokens are transferred into a verifiably non-spendable address and lose value over time, encouraging miners and promoting regular activity by them instead of one-time, potentially malicious early investments [24].

- **Practical Byzantine Fault Tolerance (PBFT)** - designed to be able to handle byzantine faults. A three-phase process requires a node to receive votes from 2/3 of the other existing nodes on the network [9]. This algorithm helps in preventing spoofing and to detect altered messages sent from malicious nodes.

Changes in the Blockchain consensus algorithm can originate something referred to as a fork. A fork is a split in the Blockchain which often occurs due to disagreements in the protocol at use. When developers propose or implement changes to the network, there is a probability that some of the nodes will not agree with the changes or even want to follow them as they go live on the network. When the community cannot decide on a single option, the need for a fork arises.

There are two different kinds of forks, **Soft Forks** and **Hard Forks**.

- **Soft forks** are the changes in which miners are not forced into updating the version of the Blockchain they are running as the changes are backwards compatible, meaning that blocks written by newer versions aswell as the ones written by older versions are all valid, despite being different. This is good as miners are not forced into any updates and the Blockchain does not need to be split in two. It won't however allow for big or drastic changes, as there is the requirement of compatibility between all of the nodes [27].
- A **Hard fork** on the other hand requires every node in the system to update the version of the Blockchain they are running as the new version brings forth comprehensive changes which prevent backwards compatibility [43]. The refusal to update software from miners will prevent them from accessing the network again and can originate a split in the Blockchain as happened to Bitcoin, originating Bitcoin Cash.

2.1.3 Smart Contracts

> "A smart contract is executable code that runs on top of the blockchain to facilitate, execute and enforce an agreement between untrusted parties without the involvement of a trusted third party" [8].

Smart contracts are essentially digital contracts executed by themselves when precise circumstances are met and can be developed and implemented on top of a Blockchain. The contract works by following simple conditions written into code. Once an entity meets the requirements and has been verified, the action stated by the contract will be executed. After these actions are processed, they're stored in the Blockchain, becoming immutable and being only available for the two intervenient parties to see. To establish a contract, it is necessary for participants to decide on how the data from the transaction will be represented and it is necessary to explore exceptions. These contracts allow other entities to basically create Decentralized Applications (Dapp) on top of an existing Blockchain and are usually an essential asset to a Blockchain given the possible value these applications can bring to the network. Adding to that, this process can help companies save resources as the process is now computarized, meaning that there is no need for a person to do it manually. However, these contracts need to be analyzed and designed carefully as each contract can introduce possible vulnerabilities into the network by allowing for exploits with the information that can be accessed through the network.

2.1.4 Technology

When talking about DLT, a common mistake for people is to think that it is the same as Blockchain. On the other hand, all Blockchains are distributed ledgers, but not all distributed ledgers are Blockchains. A Blockchain instance is a distributed ledger, but it is only a subset of distributed ledgers. This section will focus on exploring different types of DLT the way data is stored in each of them, as well as some of the advantages and disadvantages related to each type.

Blockchain

In a centralized relational database, it is expected to have tables defining different types of data, each table having their own entries. In Blockchain however, we stray away from that approach and store information in blocks which are connected, creating the chain. Since the information is chained depending when it was inserted into the chain, the order of the blocks matters, especially when used to store monetary transactions, such as in Bitcoin, one of the most commonly known examples.

In this case, the type of data ends up giving name to the type of DLT, as the group of linked blocks is named Blockchain. These blocks possess a very specific structure, being divided in Header and Body. The block header is identified by a unique hash which represents that block, aswell as the hash used to represent the previous block, defining a chain as blocks are inserted. Since the Blockchain needs an initial block to start, there is one and only one block who doesn't contain the previous block's hash and this is called the Genesis block. There is another important piece of information contained in the header, which is the Merkle Tree Root Hash, which points to the root of the Merkle Tree. The Merkle Tree, also known as a binary hash tree is an efficient way to store information [30] given that it helps with eliminating duplicate or repeated information, it reduces the amount of space needed to store transactions and due to its root hash, can help validate the integrity of the stored data .

Directed Acyclic Graph

A Directed Acyclic Graph(DAG), is another variation of a DLT where each transaction is individually uploaded and validated, saving time as there is no block to be build and there is no need for the election of who writes the next block, usually decided by the consensus mechanism [32].

The paradigm enables many transactions to be validated simultaneously because each node might have multiple parent roots, decreasing the amount of time needed for the information to be validated, compared to Blockchain technology, for example. Each new transaction in a directed acyclic graph must reference prior transactions before being accepted into the network. Each vertex in a DAG represents a transaction. Because there are no blocks, mining is not required. Then, as previously indicated, proof-of-work tasks are performed to validate previous transactions and prevent spam whenever a node makes a transaction. Transactions with a longer branch of previously validated nodes will be more likely to be approved. The fundamental distinction between a DAG and a Blockchain is that a DAG can reference numerous transactions at once, whereas a Blockchain can only reference one at a time [12].

Hashgraph

The Hashgraph approach utilizes the previously shown Directed Acyclic Graph(DAG) but instead of using a consensus mechanism like the typical Blockchain, it uses gossip about gossip and and Virtual Voting, meaning that every node helps decide the approval of information. These methods allow the network to maintain connectivity and consensus [10].

The concept of distributed ledger technology is enticing because it eliminates the need for an intermediary party. A distributed ledger, unlike Blockchain, does not require a block-based data structure. A distributed ledger is just a database that spans numerous locations, regions, or participants.

Although DLT offers this variety of options, the work developed will shine light on Blockchain technology as it was the one deemed more appropriate for this specific scenario, therefore, details noted from now one will most likely be specific for Blockchain.

2.1.5 Common Applications

Bitcoin (BTC)

Bitcoin is a decentralized and distributed network invented by Satoshi Nakamoto in 2008 [20]. It's the first and most known example of a public Blockchain. Each computer connected to the network is considered a node, and due to the public nature of the Blockchain, each of these can access the information and interact with the network freely. These nodes are called miners, and they compete through a consensus mechanism, Proof-of-Work(PoW), which consists of a computationally difficult problem, in order to decide who will write the next block of the chain. The chosen user is rewarded with an amount of Bitcoin, which has been mined. This method, although efficient, expends a lot of energy and computational resources.

Ethereum (ETH)

> "Ethereum is open access to digital money and data-friendly services for everyone – no matter your background or location. It's a community-built technology behind the cryptocurrency ether (ETH) and thousands of applications you can use today." [4].

It consists of a Blockchain created by Vitalin Buterin in 2015. As many of the public Blockchains, it used to be based on a PoW consensus mechanism, which was changed into a PoS after the Casper update in late 2020. This platform allows users to use it for small fees payed in ether (ETH). This is due to the implementation of smart contracts and the existance of the Ethereum Virtual Machine (EVM), which allows applications to run on the ethereum platform.

Fantom (FTM)

Fantom is an open source Directed Acyclic Graph (DAG) platform, which allows users to build decentralized applications (dApps) which are compatible with other Distributed Ledgers, such as Chainlink, The Graph and even with Ethereum, running on EVM. The platform takes advantage of the Byzantine fault tolerance (BFT) consensus mechanism, achieving an asynchronous version which they named the Lachesis consensus [5]. This allows for all of the upsides known to the BFT mechanism, aswell as faster processing of transactions, which are confirmed in 1-2 seconds, the avoidance of a "leader which could play a special role in the production of blocks and the ability for users to process comands at different times, due to the mechanism being asynchronous.

Avalanche (AVAX)

Avalanche is an open-source platform for developing decentralized finance apps and enterprise Blockchain installations in a scalable and interoperable environment. Avalanche allows developers to establish unique Blockchain networks with complicated rulesets, as well as build on existing private or public subnets [39]. AVAX uses the PoS consensus mechanism, which makes people who hold a lot of coins the most likely to write new blocks.

2.2 Non-Fungible Tokens

Before defining Non-Fungible Tokens, there is the need to define tokens in general. "Tokens are a digital asset defined by a project or smart contract and built on a certain Blockchain" [14]. Tokens can have several types such as reward tokens, currency tokens, utility tokens, security tokens or even access tokens.

Fungible entities, from an economic point of view refer to a certain asset with a set value which can be interchangeable with other assets or goods of the same value. One good example of this is a dollar. Dollar bills are all the same, they are all worth the same and trading one dollar bill for another should not make a difference to the person who possesses it [15].

A non-fungible asset however has no inherent value, in fact, their values is derived from the assets or goods that they represent and is usually dependant on people. A non-fungible asset will have the value a person thinks it has meaning it might be useless for one individual, but another might pay great prices for it, just like a painting would.

2.2.1 Definitions

Non-Fungible Token refers to digital assets that cannot be interchanged for another asset of the same type. Non-fungible assets, are unique and cannot be replaced. Anyone can make copies or replicas of this token, but one could never actually have another asset that is equal to the token in question. We can compare it to a painting such as the Mona Lisa or The Scream. In the same way that a painting is unique, NFTs represent information or data in a unique manner, where the holder has proof of ownership. NFT's data and the user's ownership can be verified by the Blockchain, establishing NFTs verifiable digital scarcity and the uniqueness of each asset [15].

2.2.2 Standards

The Ethereum Blockchain was the pioneer in NFT technology [25], having the first one been minted in 2015. Due to this, the most known token standards were all based around this network and developed on top of it, especially in the early days. There are three primary standards for creating tokens in the Ethereum network. These are the **ERC-20**, **ERC-721**, and the most recent and probably most optimized **ERC-1155**. ERC stands for Ethereum Request for Comment and is an official protocol for proposing improvements into the Ethereum network, where the number is the proposal identifier.

The ERC-20 standard was the one used to create the first-ever NFT in Ethereum. It can, however, be used to develop Fungible Tokens as some cryptocurrencies such as Maker (MKR), Binance Coin (BNB), and Basic Attention Token(BAT) use this standard. This token standard allows for these to be used within the network and to be exchanged between addresses as use of specific decentralized applications implemented on the Ethereum chain [25].

Although ERC-20 was the first standard to be used, ERC-721 was its first upgrade, creating a standard that was focused on the uniqueness of NFTs. Every token made with this standard is unique and is also wholly traceable using Etherscan [33]. These provide the owner proof of ownership and authenticity, as all of them can be checked digitally, ensuring that a particular user really does own that unique asset. There is also the possibility to check the history of all the users that have owned that same token.

Lastly, ERC-1155 was developed on Ethereum but by the Enjin team. Enjin is a token on the Ethereum platform, and the project is based around facilitating the use of NFTs in various areas such as games [19]. In this same context, the team developed a standard in which multiple tokens, both Fungible and Non-fungible, could be handled by a single, smart contract in order to reduce computational overhead. The standard identifies common code and stores it, preventing its repetition and reducing the storage expended by those tokens as well as reducing gas fee prices which would be wasted on processing the same code multiple times. This also allows for multiple tokens to be transferred in a single transaction, with a batch mode, resulting in lower costs alongside better overall transaction speed and network efficiency [34].

2.2.3 Properties

There are certain properties required for a token to be considered an NFT. Contrary to fungible tokens, NFTs are not divisible. Although a single cryptocurrency for example is divisible into decimal points, which you can acquire and trade, an NFT is a singular asset that can not be cut in half or be divisible in smaller portions.

Also unlike fungible tokens, NFTs can be restricted through their smart contract, limiting or even preventing the transfer of that same token. This means that a token can be made into a personal item, which justifies the hypothesis that these tokens can be used as identifiers of some sort, which can never be transferred or sold. The same smart contract that restricts the token can grant it properties which will remain the same as long as the contract does as well. The smart contract will contain a set of properties which will define the token after it is minted [44].

Finally, an NFT can serve as an absolute proof of ownership, which may serve as proof of authenticity as well. As indicated previously, an NFT always has an owner and that can be verified online through the network's page, meaning one can use this to prove that asset belongs to them as long as that person has access to the address which possesses the token. In certain contexts and given that the interchangeability of these tokens can be limited, this can essentially serve as a proof that the information contained in the token is authentic, be what it may be.

2.2.4 Common Applications

As previously presented, NFT use cases are mostly in the digital art context, some of which being:

The Bored Ape Yacht Club

> "BAYC is a collection of 10,000 Bored Ape NFTs - unique digital collectibles living on the Ethereum Blockchain. Your Bored Ape doubles as your yacht club membership card, and grants access to members-only benefits." [31].

The BAYC is currently one of the most sold collection and one that has been responsible for some of the biggest NFT purchases in these recent years. It also serves as an example of how NFTs can be used as a means to authenticate a user into a certain system, in this case, the Yacht Club.

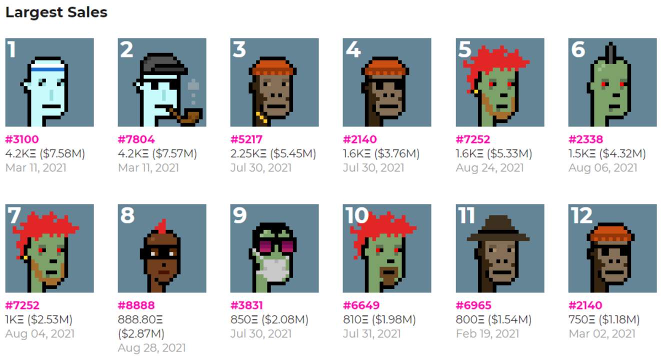
Figure 2.3: Bored Ape Yacht Club

Crypto Punks

Although not the first NFT collection being sold on the Ethereum Blockchain, Crypto Punks is a collection of 10,000 24x24 pixel art images which possess 87 attributes, also known as traits [42]. Each "punk" can have up to 7 attributes and each combination is never repeated, making them unique. This project started off without any clear view, being just a set of unique digital art pieces, but over the years it has garnered a lot of attention and become one of the most influential NFT collections.

The Sandbox

The Sandbox is and Ethereum based decentralized NFT metaverse. The project is essentially a digital world where players can own pieces of land or even in game assets, which are all stored as NFTs [38]. All of the assets are stored in a Blockchain and have specific owners, which are players of the game itself. This project combines the usage of the 3 mentioned NFT standards. Transactions and interactions in the game come in the form of ERC-20 tokens, pieces of unique purchasable land in-game are all supported by the ERC-721 standard and, last but not least, user generated content using the game's Game Maker feature, which can be traded in the marketplace are all made using ERC-1155.



Largest Sales

1
#3100
4.2KΞ ($7.58M)
Mar 11, 2021

2
#7804
4.2KΞ ($7.57M)
Mar 11, 2021

3
#5217
2.25KΞ ($5.45M)
Jul 30, 2021

4
#2140
1.6KΞ ($3.76M)
Jul 30, 2021

5
#7252
1.6KΞ ($5.33M)
Aug 24, 2021

6
#2338
1.5KΞ ($4.32M)
Aug 06, 2021

7
#7252
1KΞ ($2.53M)
Aug 04, 2021

8
#8888
888.80Ξ
($2.87M)
Aug 28, 2021

9
#3831
850Ξ ($2.08M)
Jul 30, 2021

10
#6649
810Ξ ($1.98M)
Jul 31, 2021

11
#6965
800Ξ ($1.54M)
Feb 19, 2021

12
#2140
750Ξ ($1.18M)
Mar 02, 2021

Figure 2.4: Crypto Punks [42]

2.3 Applications for DLT and NFT in the medical field

The medical field has been pointed out in multiple occasions as one of the fields that could possibly serve as a testing field for both DLT and NFTs, being often mentioned to be one with the possibility for applications based on them. Although some ideas are still just suggestions and have no work to back them up, there are also some which are in current development and may shine light to these possibilities in the near future.

2.3.1 Blood Banks

One of the suggested ideas as other scenarios we're pondered for NFT, was a digital bloodbank, recorded on a Blockchain [2]. Basically, each donation would be registered and recorded in the Blockchain, generating an NFT which would uniquely identify the blood sample and its information. This would in turn allow healthcare facilities to have a database of available blood samples, which could be consulted and improve traceability of the blood samples aswell as a simplification in the delivery process whenever needed.

2.3.2 Safe Prescription

Following the blood bank idea, the safe prescription is a slightly different idea from the previous one applied to the pharmaceutical field. Although it's not the most common of events, during the delivery proccess, some medicine may go missing from a batch of drugs [16]. The idea would be to tag each batch or even box of medicine with an NFT acting as an identifier. Once this was done, distribution would become easier and, as in the previous case, traceability would become much easier. Besides that, these tokens could also act as an authenticity check for pharmacies and hospitals.

2.3.3 Aimedis

> "Aimedis was founded in 2016 by the practicing physicians Michael J. Kaldasch and Ben El Idrissi, who have been working in Internal Medicine and Neurology for over

Figure 2.5: The Sandbox [3]

> 12 years. The idea was born during their time spent in the ER and ICU while searching for vital patient medical history." [1].

With the recent concept of the metaverse, Aimedis decided to pursue an approach that would connect healthcare to that metaverse, aiming for transparency, trust and interoperability when regarding medical data. Their goal is to allow the user to tokenize his own health data and keeping it on the network as a way to better control it and share it as the patient/user sees fit [7]. This could entail just sharing with a healthcary professional for diagnosis purposes or even to share or sell an anonimized version of their patient details to serve as data pools for healthcare and science.

2.4 Chapter Summary

Based on the information gathered and researched, it is safe to assume that the technologies in question pose a theoretical alternative to the current storage of medical data. Such conclusion is based on the fact that not only is there a prototype in a similar use case, but there is also a plethora of similar suggested use cases in healthcare which validate their importance and possible utility. Therefore prototyping and stress testing this specific use case seems to be a worthwhile contribution in the area.

Chapter 3

Blockchain and NFT in Healthcare

3.1 Problem Statement

Recent studies have shown that storage of medical information is redundant and inefficient. Files are sometimes duplicated or lost leading to redundant medical testing or even misdiagnosis due to lack of access to previous medical records. Diagnosis can also be a problem if a patient has either moved or is travelling, lacking access to previous records, due to them being stored locally for each entity. Centralized storages also present with possible single points of failure, which might reduce availability due to any technical issue, or malicious attack.

The fact that patients have no control over their own information or how it is being managed also leads them prone to having their identity exposed or shared without their consent.

3.2 Solution Perspective

The proposed solution is based on the creation of personal NFTs per patient, which would contain previously obtained medical records and would be uploaded anytime the patient presented in a healthcare facility, with the information generated by the appointment or medical exams.

The NFT acts as a proof of ownership over the information accessible through it, making the patient be in control of its own data and allowing it to be shared only at its command.

The fact that data is associated to an NFT means that it would have to be stored in a Blockchain which would support not only smart contracts, but NFT minting aswell. Due to the nature of a Blockchain, this information would be encrypted by the appropriate cryptographic methods but would be replicated over various nodes of the network.

3.3 Validation and Expected Results

The first step in validating the suggested approach is having a working Blockchain which supports smart contracts, allowing NFT's to be deployed based on the information stored in that same network. There are several characteristics to the Blockchain which can be altered in order to make it more or less suitable to the use case in hand, such as the type of Blockchain or the consensus mechanism which selects a node to write the next block of information.

After testing the multiple variables on the network and achieving the more suitable one, there was the need to test other technologies which were chained together to make the prototype flow in the intended manner.

3.4 Work Proposal

In an initial stage, the objective was familiarizing ourselves with the hands-on approach to the technologies at hand, both Blockchain specifically as well as how to produce NFT's and how to play around the access to their information. It's important that around halfway through the developing period, some initial tests are conducted in order to rule out certain problems from the prototype, allowing it to be changed and hopefully improved , in order to produce the best results possible. After collecting all of the data necessary, conclusions were made considering the benefits and weaknesses of the prototype and highlighting future changes and improvents that can eventually be made.

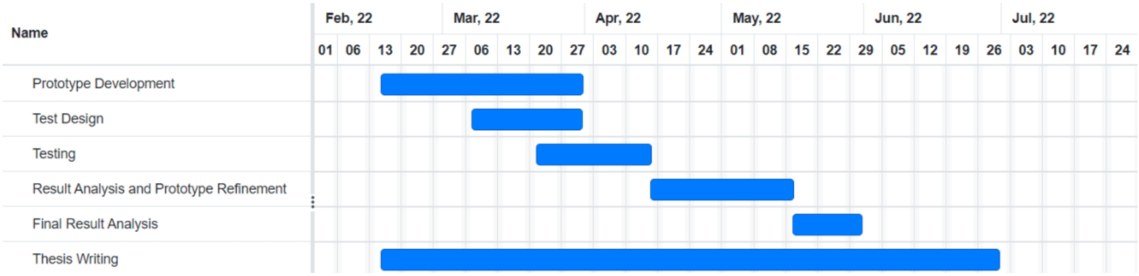


Figure 3.1: Work Plan

Chapter 4

Implementation

Researching about the topic, there were a couple of topics which had to be decided upon to make the prototype flow and of better value. Besides deciding in which network the contract would be deployed, there was the need to choose how the data was going to be stored, whether it would be encrypted, whether each NFT would be a single file or if and NFT could hold all of our information at once, what information to keep on the metadata. All these topics were important to consider before attempting an implementation but should also be taken into account and reconsidered during the implementation, in case something requires changes in approach.

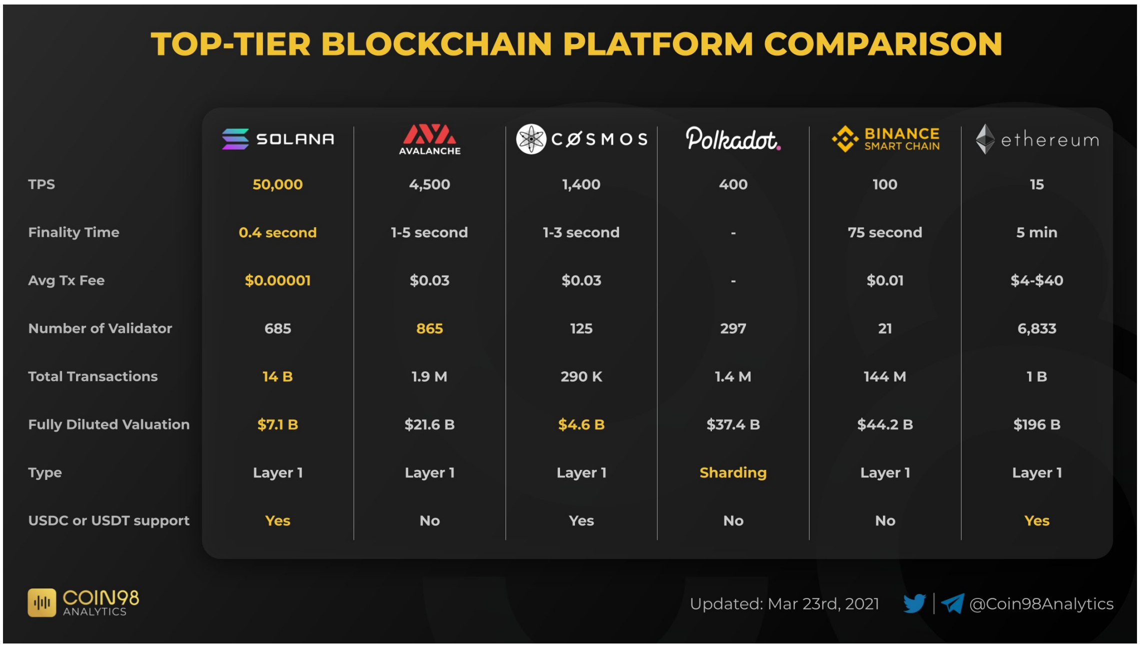
Sections 4.1, 4.2, 4.3 and 4.4 cover the technologies that were integrated in the prototype during development and implementation, focusing on what each specific one contributed to and why they were chosen to be used. Following that, section 4.5 describes in more detail what was developed and how the previously referred technologies were chained into a functioning prototype. Finally, section 4.6 presents a summary of this chapter contents.

4.1 Ethereum

There is an increasing amount of blockchains which support smart contracts and NFTs but each has its own implementation, meaning not all work the same nor do they require the same effort and therefore not all are suitable for the use case in question.

After researching through these options, the list was reduced to just a handful of networks which provide what was needed for the prototype. Out of the large and very general list of what chains support NFTs, some options were obvious options such as Ethereum, Polygon and Avalanche. Besides considering a list of factors such as transaction speed, transactions per second (TPS), costs of transactions and mean time for transactions, there was also a need to look into how easy it would be to build something based on these chains' smart contract system and token generating methods (see figure 4.1).

Be it because of simplicity of the processes, but also the amount of resources available for each individual option, there is a need to compare and assess which platform provides the most support and facilitates development. It is a well-known fact that Ethereum is the pioneer in these areas,



TOP-TIER BLOCKCHAIN PLATFORM COMPARISON

	SOLANA	AVALANCHE	COSMOS	Polkadot.	BINANCE SMART CHAIN	ethereum
TPS	50,000	4,500	1,400	400	100	15
Finality Time	0.4 second	1-5 second	1-3 second	-	75 second	5 min
Avg Tx Fee	$0.00001	$0.03	$0.03	-	$0.01	$4-$40
Number of Validator	685	865	125	297	21	6,833
Total Transactions	14 B	1.9 M	290 K	1.4 M	144 M	1 B
Fully Diluted Valuation	$7.1 B	$21.6 B	$4.6 B	$37.4 B	$44.2 B	$196 B
Type	Layer 1	Layer 1	Layer 1	Sharding	Layer 1	Layer 1
USDC or USDT support	Yes	No	Yes	No	No	Yes

COIN98 ANALYTICS

Updated: Mar 23rd, 2021 @Coin98Analytics

Figure 4.1: Network comparison according to Coin98 Analytics

meaning that, as expected, it also possessed the largest amount of tools and support for developers to experiment and navigate possibilities within the chain as well as an already large amount of other developers attempting projects, which leads to more information available on what works and why some approaches are better than others. There are however concerning factors such as the cost of each transaction and how many of these can be processed per second. Ethereum is known for having some of the highest prices for transactions, which are very well known in the NFT art world, due to the fees that any user acquiring an NFT must pay. It is also public that Ethereum's transaction speed and number of TPS are not the best when comparing to the new options that have surfaced in the past years.

Contrasting to these perspectives, both Solana and Avalanche present much lower fees and better values for transaction speed and TPS which would certainly improve performance and reduce costs in a system as the one we're attempting to develop. Despite all these advantages, upon diving into their environments, the difference between them and Ethereum was very noticeable when regarding NFTs. Despite being relatively big chains which support this technology, the quality of the tools available and the amount of feedback from other developers was comparatively much lower than what was available for the Ethereum network. There is also one more upside to developing in Ethereum opposed to these 2 big competitors which is the fact that Polygon is completely compatible with an Ethereum smart contract. This means the possibility to take advantage of Ethereum's developer environment and tools, while improving considerably on the costs and transactions side of things.

As for other options such as Flow, despite the user-friendly tools available, there are very few developers who have already fully used this system, when comparing to other options, which would require more time invested in figuring out what works and what does not, given the contrast in the amount of feedback from this chain and the amount from bigger, more known options. Being that Flow is a less known and less grown chain also means that the number of TPS and the duration for transactions is in the middle of the pack, being reasonable, but also not being as good as desired. For simplicity purposes, the chosen platform was the Ethereum network due to the better testing environment and possibility of later on switching to the cheaper, faster and compatible option of Polygon.

4.2 IPFS via Pinata

Researching about NFTs and other authors who had already created some and marketed these digital assets, it was obvious that these tokens did not have to be specifically images. There are examples of NFTs using text files, PDF files or even GIFs or small videos.

Taking this into account, it is expected that differing file types like these can vary in size considerably, and having such files going directly on the chain when minting NFTs was likely to impact performance of the network itself due to the accumulation of data as the amount of NFTs minted increases, especially due to the high amount of clients using the network and venturing themselves in the new and innovative technology that are NFTs. This would eventually prove, not only to be detrimental to the network, but also unviable as the blockchain grows over time. The most common practice would be to store the files elsewhere, usually in a decentralized storage or some other similar type of network as the Ethereum smart contracts allow users to provide a URI instead of a file to mint the NFTs, meaning the NFT can be based on a file which is not stored directly on the chain as long as that URI is valid and attached to it. The data stored in an NFT is usually divided in 2 parts.

The file being stored, which can usually vary in size and type and then, there is usually a metadata file, which contains important information about the content and usually contains a URI to where this content is stored. This metadata file is usually the one attached to the NFT when minting, as it contains all the information that an NFT contains. It is important to note that these must be stored in a secure place, not only for the safety of the files but for their availability. Since the smart contract receives a token URI, it is common for smaller NFT creators to mint tokens which eventually have no content and are not even accessible because the files are no longer existent in the storage they were at during the time of the minting. This serves to highlight how critical the storage process is to the whole NFT production process.

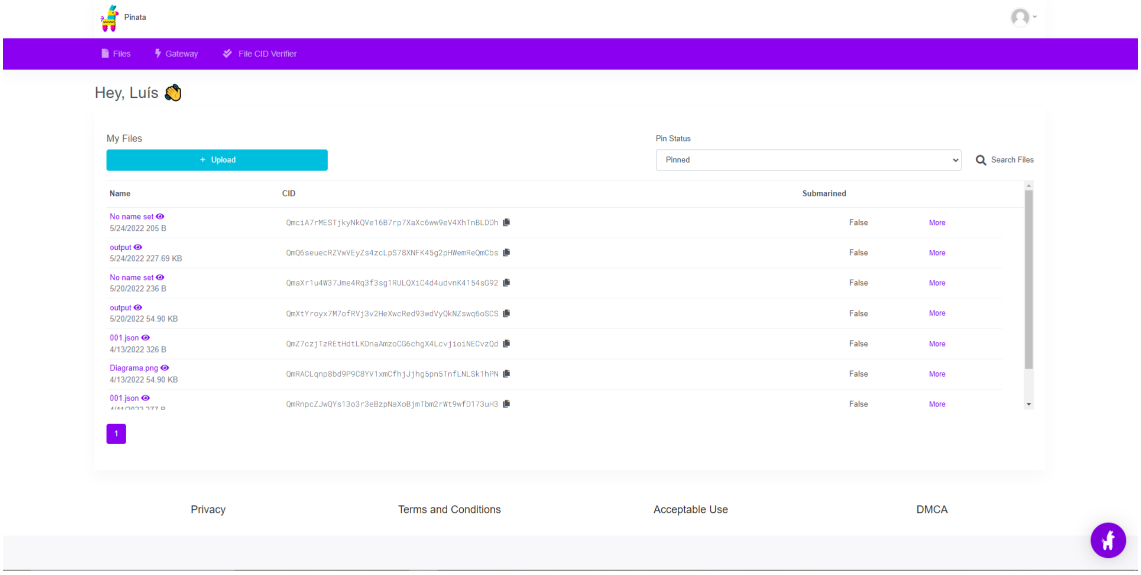
The InterPlanetary FileSystem (IPFS) (see figure 4.2) is a peer-to-peer network used for storing and sharing data and is used as a protocol for some of the currently existing decentralized solutions. Using the IPFS, we can store both the NFT content and the corresponding metadata and then attaching the resulting URIs to the NFT when calling the method from the developed smart contract.

Despite the IPFS being usable on its own, one tool which proved to be very useful was the Pinata API (see figure 4.3). This API not only allowed the prototype to directly upload the selected

IPFS powers the Distributed Web

A peer-to-peer hypermedia protocol
designed to preserve and grow humanity's knowledge
by making the web upgradeable, resilient, and more open.

Figure 4.2: InterPlanetary FileSystem



Hey, Luís 👋

My Files

Pin Status: Pinned

Name	CID	Submarined	
No name set 5/24/2022 205 B	QmciA7rMESTjkyNkQVe16B7rp7XaXc6ww9eV4XhTnBLDDh	False	More
output 5/24/2022 227.69 KB	QmQ6seuecRZVwVEyZs4zcLpS78XNFK45g2pHWemReQmCbs	False	More
No name set 5/20/2022 236 B	QmaXr1u4W37Jme4Rq3f3sg1RULQXiC4d4udvnK4154sG92	False	More
output 5/20/2022 54.90 KB	QmXtYroyx7M7ofRVj3v2HeXwcRed93wdVyQkNZswq6oSCS	False	More
001.json 4/13/2022 326 B	QmZ7czjTzREtHdtLKDnaAmzoCG6chgX4LcvjioiNECvzQd	False	More
Diagrama.png 4/13/2022 54.90 KB	QmRACLqnp8bd9P9C8YV1xmCfhjJjhg5pn5TnfLNLSk1hPN	False	More
001.json 4/11/2022 277 B	QmRnpcZJwQYs13o3r3eBzpNaXoBjmTbm2rWt9wfD173uH3	False	More

Figure 4.3: Pinata Dashboard

file and its corresponding metadata into the IPFS, but also provided a very useful dashboard which showed all the uploaded files, with dates, sized and access to their URIs, making it possible to view the files and check, especially in early stages of development, if the file was properly uploaded, if the URI used to mint the NFT was correct and if the information was properly displayed in the metadata files. Most of these utilities were no longer necessary in latter stages of the prototype development process considering the uploading part of the prototype was the first to be fully developed and that after the encryption, there is no longer the possibility to view the contents of the NFT, reducing utility of this tool as the implementation progressed. However, this tool provided, crucial feedback or the early stages, which would not be possible if simply replaced by the IPFS API.

To put it simply, the Pinata API was a tool which provided an easier and smoother testing phase of the initial prototype due to its very useful dashboard.

4.3 Moralis API

The Moralis API (see figure 4.4) is a tool which provides full-stack workflow when building dApps and is compatible with most other web3 tools and services. It is available on Ethereum, Binance Smart Chain, Polygon, Solana and Elrond, including *testnets* which makes it a very useful tool. In this particular case, the API is used as the means to fetch information from the network in question, which is the Ropsten Ethereum Testnet. Moralis has plenty of methods ranging from checking account balances to other address properties that might be reachable on chain, but the method that stood out in relevance for this prototype was the getNFT method offered by the platform.

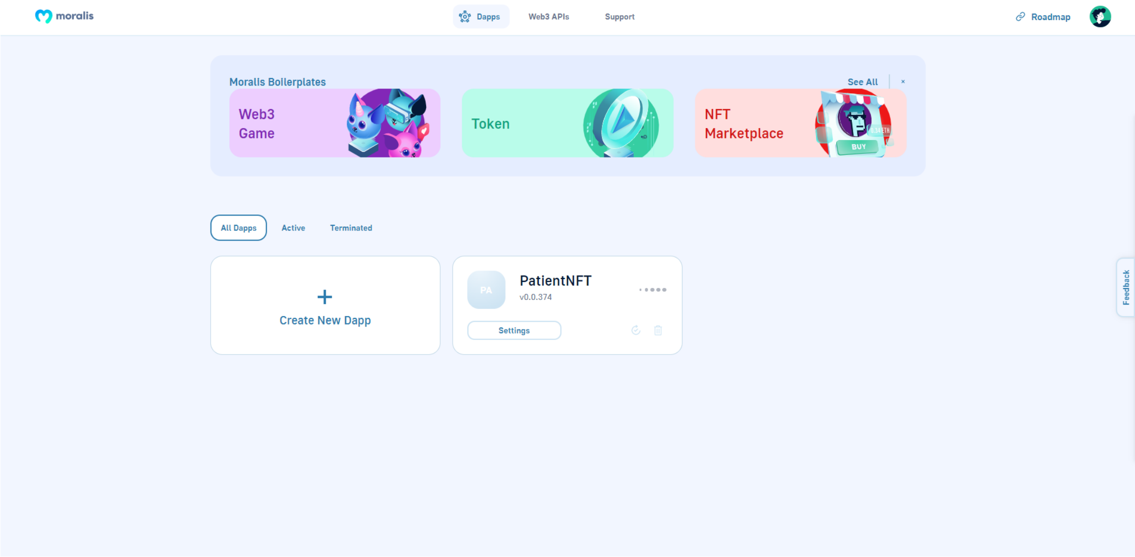


Figure 4.4: Moralis API

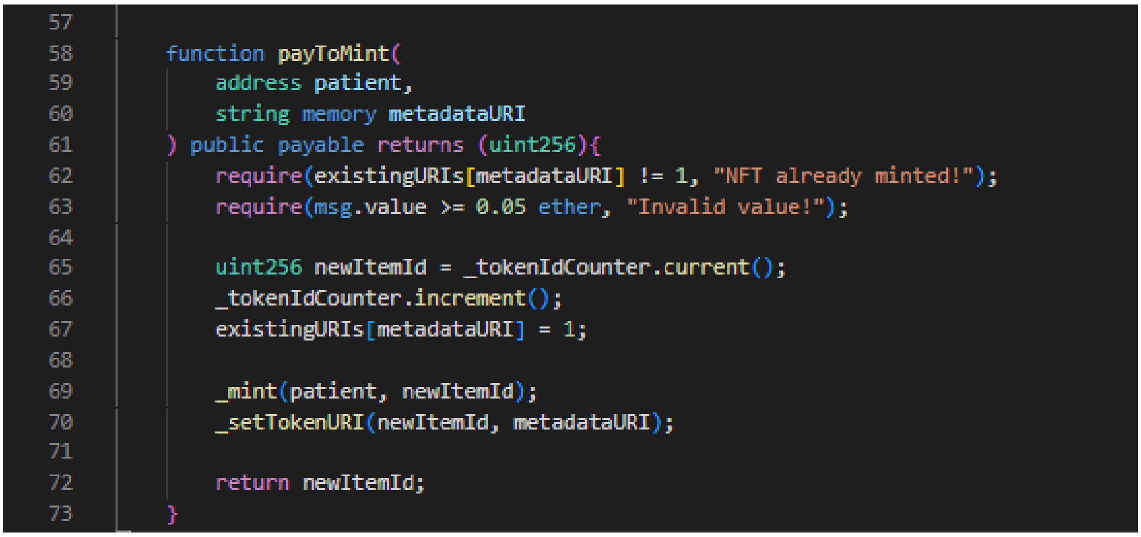
This method, as the name suggests, given an address and a chain identifier, allows anyone to retrieve information about all the NFTs owned by that address on the specified chain.

This is very useful as not only we can see the metadata, which gives us all the viewable information on the file, but we also receive the URI to the actual file contained in the NFT. If this file is public, then we can access it right away, but even if it is encrypted and secure, it can be redirected to the server, where it will be decrypted and then sent back to display it on screen. Furthermore, there is other information available when fetching the NFTs, such as IDs and transaction hashes which can help with confirming that everything is correct or even help debugging in case of errors in the process.

4.4 Smart Contract

Given that Ethereum was the selected blockchain to develop this prototype, the smart contract that was made was developed using Solidity. Solidity is a high-level programming language which is object-oriented and is used to implement Smart Contracts in the Ethereum blockchain. It is designed to target Ethereum's specific Virtual Machine, the EVM. Using this programming language and with the help of OpenZeppelin, which helps set the standard for Ethereum smart contracts and has plenty of documentation to help developers achieve what they want out of a smart contract, the result was the creation of an appropriate contract which is in compliance to good practices of what to do and what not to do when developing such a type of contract. This contract contains 3 main methods plus a couple that are standard to the contracts in general.

- PayToMint (see figure 4.5) is a method that allows a user to mint an NFT into his own address by paying a specified amount of ether.



```

    function payToMint(
        address patient,
        string memory metadataURI
    ) public payable returns (uint256){
        require(existingURIs[metadataURI] != 1, "NFT already minted!");
        require(msg.value >= 0.05 ether, "Invalid value!");

        uint256 newItemId = _tokenIdCounter.current();
        _tokenIdCounter.increment();
        existingURIs[metadataURI] = 1;

        _mint(patient, newItemId);
        _setTokenURI(newItemId, metadataURI);

        return newItemId;
    }
```

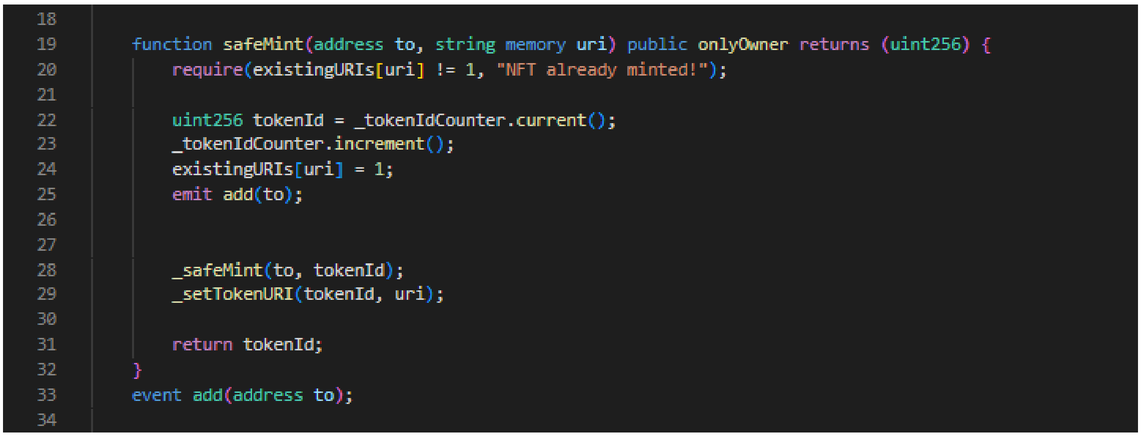
Figure 4.5: PayToMint method details

  This method would make sense in case of a user logging into his own address at the healthcare facility and paying to submit his own health files and turn them into NFTs.

- SafeMint (see figure 4.6) allows a user to mint an NFT into another specified address paying for just the fee presented by the network.

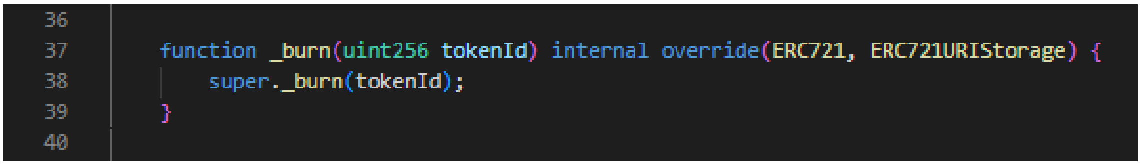
  This method is applied when the facility in question takes care of the minting process, paying for and then sending the token to the patient's address.

- Burn (see figure 4.7) allows a user to burn his own NFT (this method makes use of the onlyOwner tag in solidity, making it impossible for anyone other than the owner of the NFT to burn/delete the tokens in question).



```

function safeMint(address to, string memory uri) public onlyOwner returns (uint256) {
    require(existingURIs[uri] != 1, "NFT already minted!");

    uint256 tokenId = _tokenIdCounter.current();
    _tokenIdCounter.increment();
    existingURIs[uri] = 1;
    emit add(to);


    _safeMint(to, tokenId);
    _setTokenURI(tokenId, uri);

    return tokenId;
}
event add(address to);

```

Figure 4.6: SafeMint method details



```

function _burn(uint256 tokenId) internal override(ERC721, ERC721URIStorage) {
    super._burn(tokenId);
}

```

Figure 4.7: Burn method details

This last method is default to many contracts and exists as a sort of safety tool in case of any errors in the process that could result in a patient getting a corrupted file or any file that would pose no relevance to this patient, such as duplicates.

Between the 2 methods to mint NFTs, SafeMint was chosen to be used in the prototype: the healthcare facility would be logged on their address and would pay for the minting of the NFT and have the method mint it directly into the patient's address, which would be provided before the medical service such as a diagnostic or consultation. The hospital would pay the fee and could then include it in the final price of the consultation which would simplify the whole process for the patient. This is a better approach than having the patient pay for his own NFTs (PayToMint) as that would remove part of the authenticity of the information due to it being created by the patient. PayToMint would also require users to be in possession of Ether, an asset which is volatile and based on recent technology which most people are not familiar with. Besides the technology itself being new, a patient can be any person, meaning that the solution instanced in this prototype should be alluring to the general public despite each one technology skills. There is a large amount of people who are not familiar with technology in general, let alone blockchain technology and crypto currencies. Forcing the average person into paying for and possessing an asset which they do not grasp could easily lead to lots of problems, stemming from confusion, panic and vulnerabilities induced by the lack of knowledge or ability to handle such technologies.

Such approach would make the present solution inviable. By putting this responsibility on the healthcare facility, we are able to simplify the process for the patient and reduce stress. There would also be a possibility that such as commonly known credit card frauds, some malicious intent would be directed towards this technology, aiming to take advantage of the lack of experience and knowledge that the general public would have on such technologies, exploiting them maybe for the health data, but more likely for the asset that is Ether, which has monetary value and would therefore be a target for scammers.

4.5 Solution

Combining the technologies referenced in previous sections 4.1 to 4.4, it was possible to integrate all the distinct functionality necessary for the prototype to work as intended in the beginning of the whole process.

The prototype implementation consists of a tool which has two main functions, one to upload files (see figure 4.8) and another to list files (see figure 4.9), each using different tools and targeting different types of users and use cases.

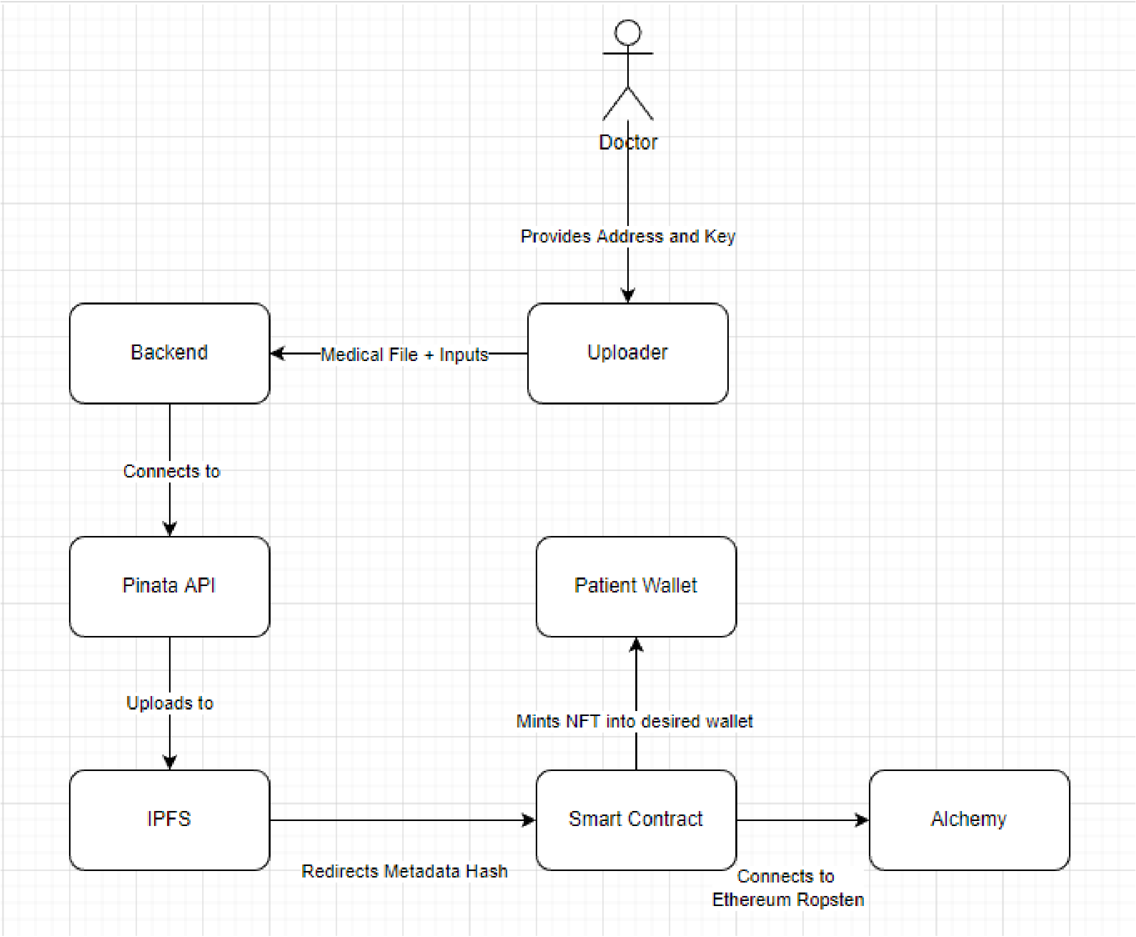


Figure 4.8: Upload Architecture

4.5.1 Upload NFTs

The uploading part of the app (see figure 4.10) is only available after a user has authenticated into the app using an administrator account. In this context of testing, the administrator account consists of an address that was created for the sole purpose of simulating a worker at a health facility accessing the app. There could be several administrators which would have to be specified to the app so it would know who was and who was not entitled to the function of uploading files.

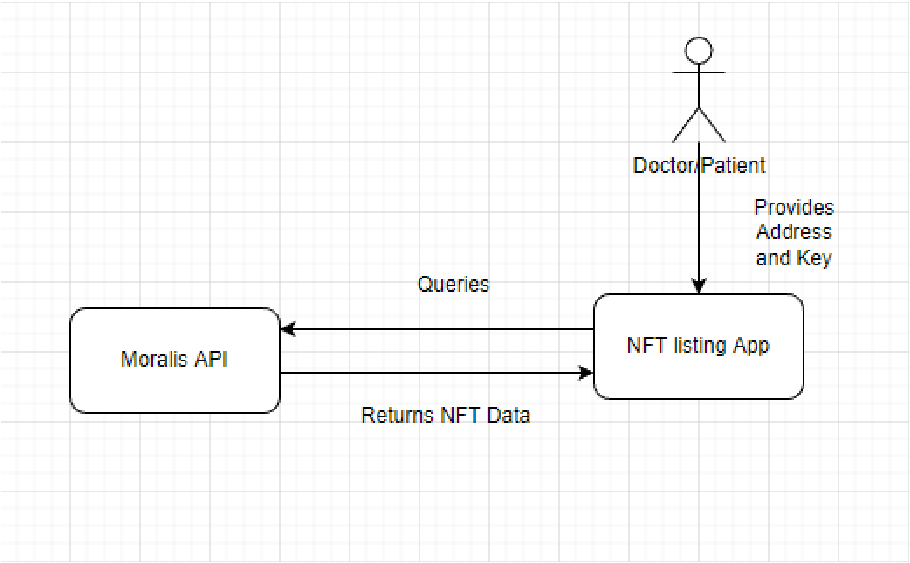
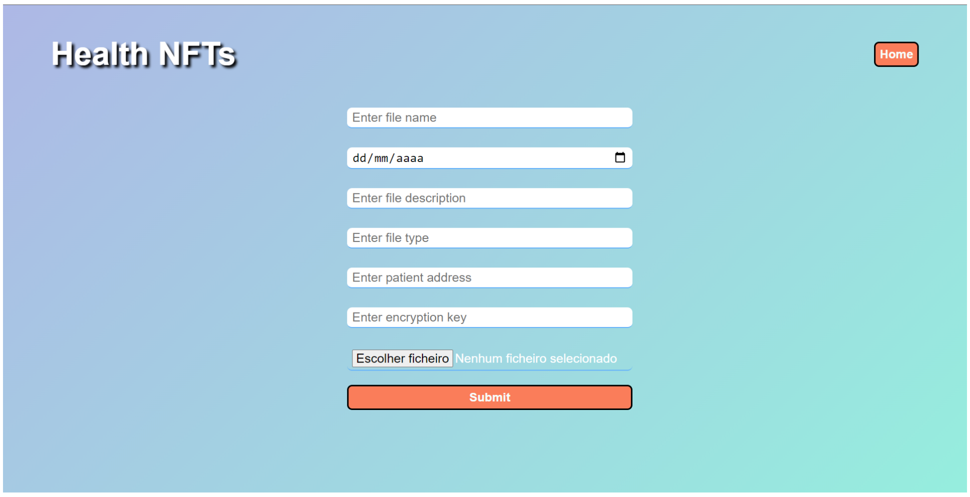


Figure 4.9: Lister Architecture

To help proceed with this authentication, there is the need for the browser extension Metamask (see figure 4.11a), which will serve as a point of connection between the administrator address and the prototype application itself.


Health NFTs

Home

Enter file name

dd/mm/aaaa

Enter file description

Enter file type

Enter patient address

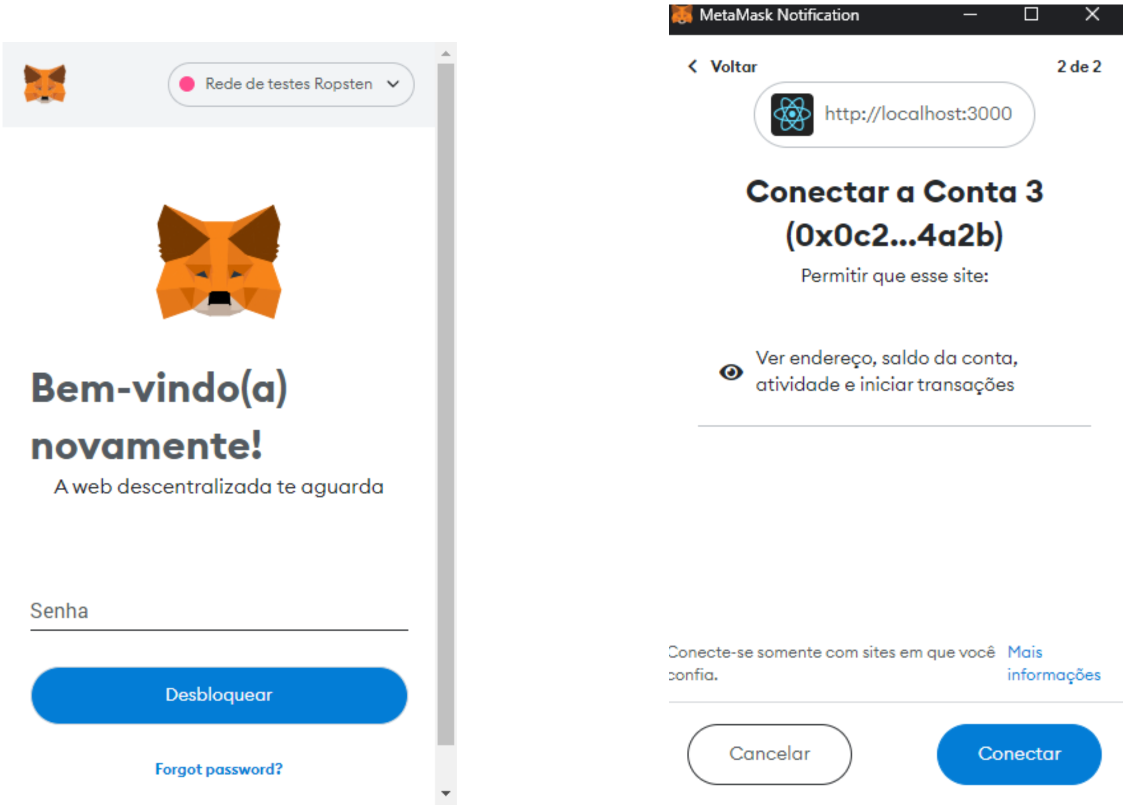
Enter encryption key

Escolher ficheiro Nenhum ficheiro selecionado

Submit

Figure 4.10: Uploading form screen

After authentication (see figure 4.11b) with an administrator account, the connect button (see figures 4.12 and 4.13) will update and the upload button (see figures 4.14 and 4.15) is visible on the main page. When the user clicks this button, it will redirect the app to a form page which requires a name for the file, a description, a date, a type of file, which refers to type of medical document being uploaded, such as an X-Ray, or a blood exam and then, a file, typically an image (but any other files if possible) so that it is easily displayed afterward and then an address to forward the



Bem-vindo(a) novamente!

A web descentralizada te aguarda

Senha

Conectar a Conta 3 (0x0c2...4a2b)

Permitir que esse site:

Ver endereço, saldo da conta, atividade e iniciar transações

Conecte-se somente com sites em que você confia.

(a) Metamask Log-in Screen

(b) Metamask pop-up when authenticating

Figure 4.11: Metamask Browser Extension)

NFT to and a key to encrypt the file with.

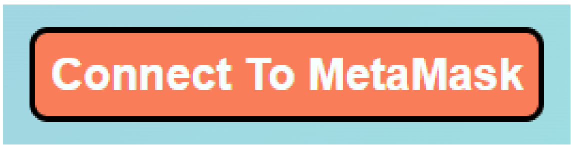


Figure 4.12: Connect button in the home page

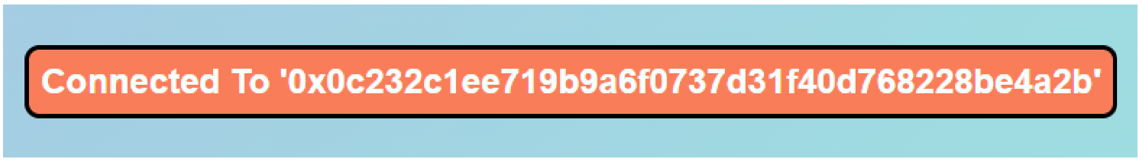


Figure 4.13: Connect button after authentication with administrator account

When the user fills and submits the form, the prototype application proceeds to encrypt the uploaded file with the provided key using a very commonly know method, the AES encryption,

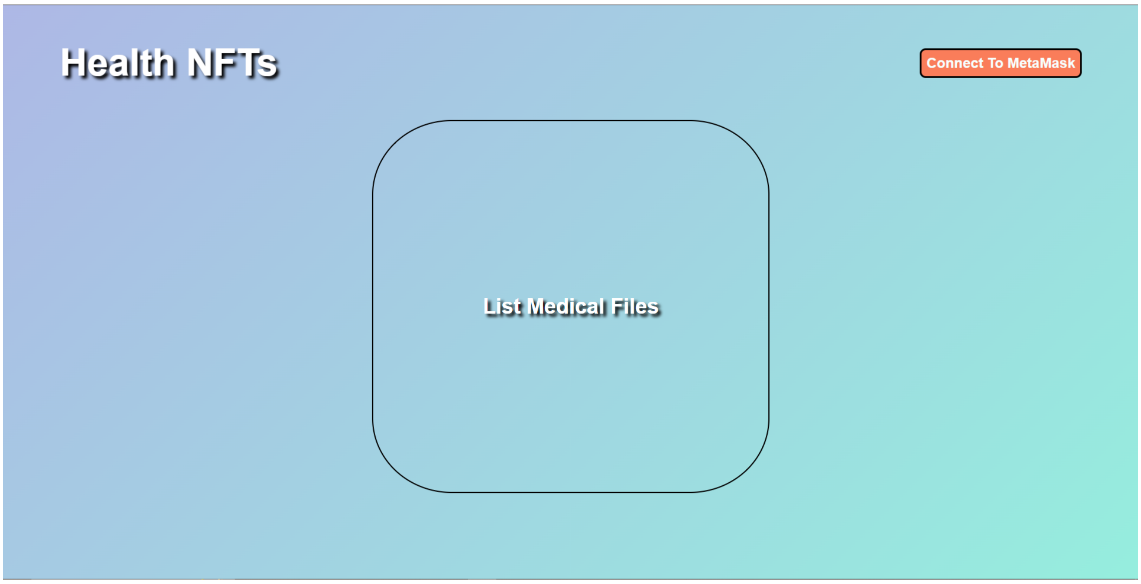


Figure 4.14: Home Screen without authentication

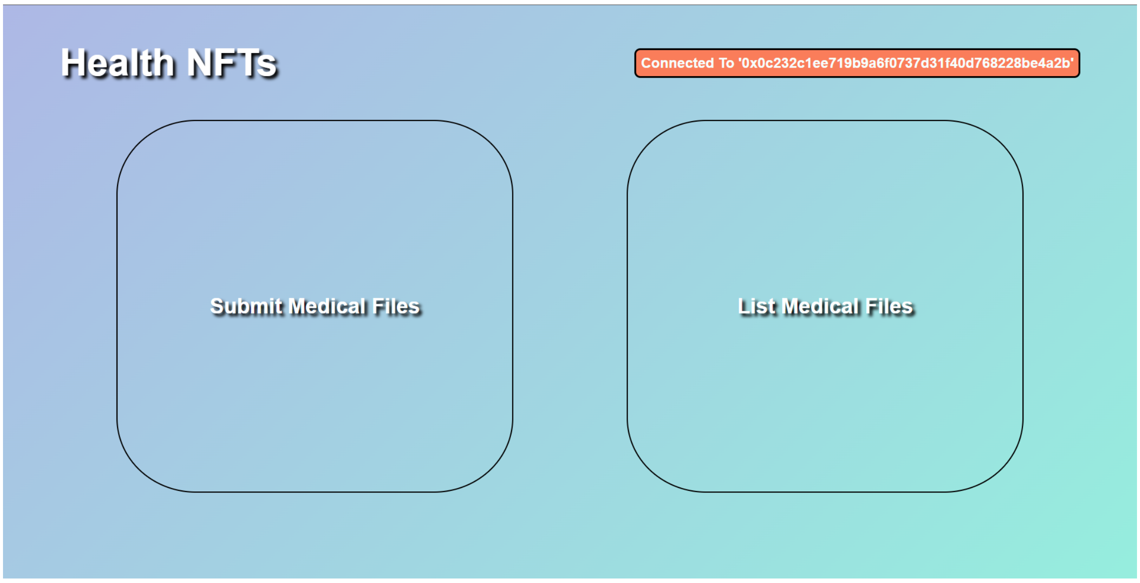
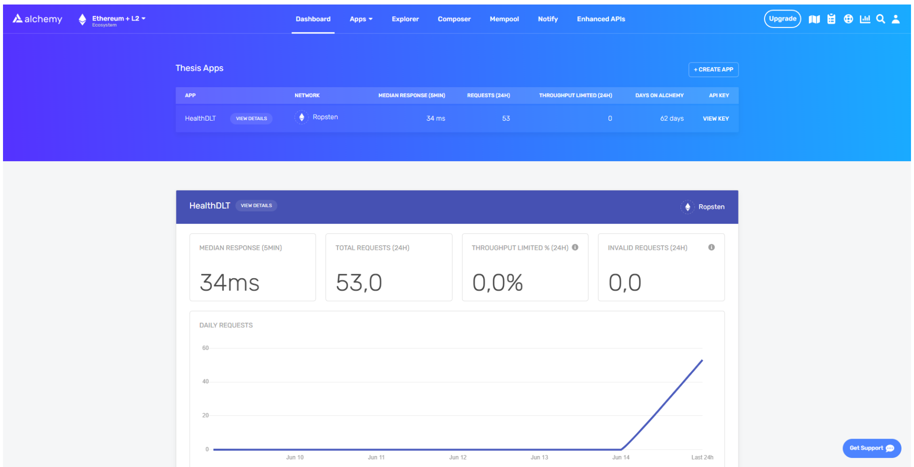


Figure 4.15: Home Screen after authentication with administrator account

then pin it on IPFS using the Pinata API. This process returns an URI, which will then, together with the rest of the information be put into a Metadata file that will also be uploaded to the IPFS.

After the server part of the prototype receives the response consisting of the metadata file URI it redirects the URI into the NFT minting function provided by the Smart Contract that was developed and deployed in the Ropsten Ethereum Testnet, creating the NFT and instantly redirecting it to the address that was provided where it will be available in 30 minutes.

The connection to this network was made using servers hosted by Alchemy(see figure 4.16) which is a platform that provides tools to assist in development of dApps and encourage Web3 development. Alchemy was considered the better choice since it allows access to the network, and to take a look into relevant information and statistics about the prototype application (see figure 4.17).



Thesis Apps

APP	NETWORK	MEDIAN RESPONSE (5MIN)	REQUESTS (24H)	THROUGHPUT LIMITED (24H)	DAYS ON ALCHEMY	API KEY
HealthDLT	Ropsten	34 ms	53	0	62 days	VIEW KEY

HealthDLT Ropsten

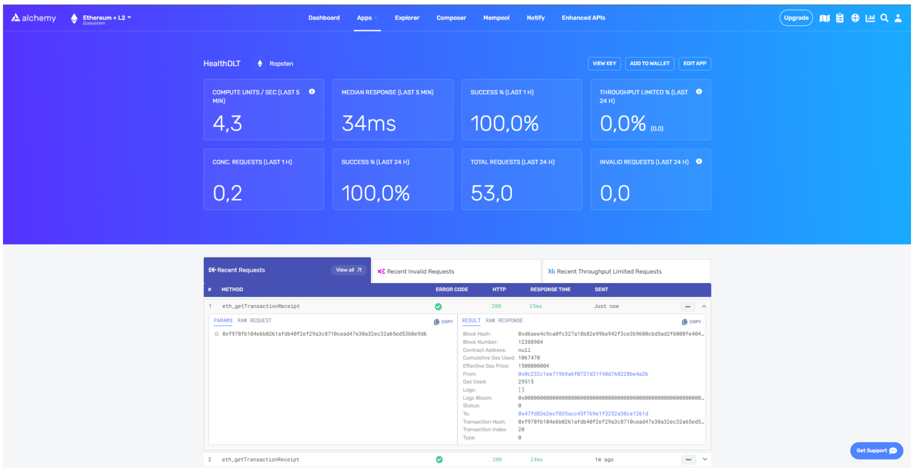
MEDIAN RESPONSE (5MIN): 34ms

TOTAL REQUESTS (24H): 53,0

THROUGHPUT LIMITED % (24H): 0,0%

INVALID REQUESTS (24H): 0,0

Figure 4.16: Alchemy Dashboard



HealthDLT Ropsten

COMPUTE UNITS / SEC (LAST 5 MIN): 4,3

MEDIAN RESPONSE (LAST 5 MIN): 34ms

SUCCESS % (LAST 1 H): 100,0%

THROUGHPUT LIMITED % (LAST 24 H): 0,0% (0,0)

CONC. REQUESTS (LAST 1 H): 0,2

SUCCESS % (LAST 24 H): 100,0%

TOTAL REQUESTS (LAST 24 H): 53,0

INVALID REQUESTS (LAST 24 H): 0,0

#	METHOD	ERROR CODE	HTTP	RESPONSE TIME	SENT
1	eth_getTransactionReceipt	✓	200	25ms	Just now
2	eth_getTransactionReceipt	✓	200	24ms	1m ago

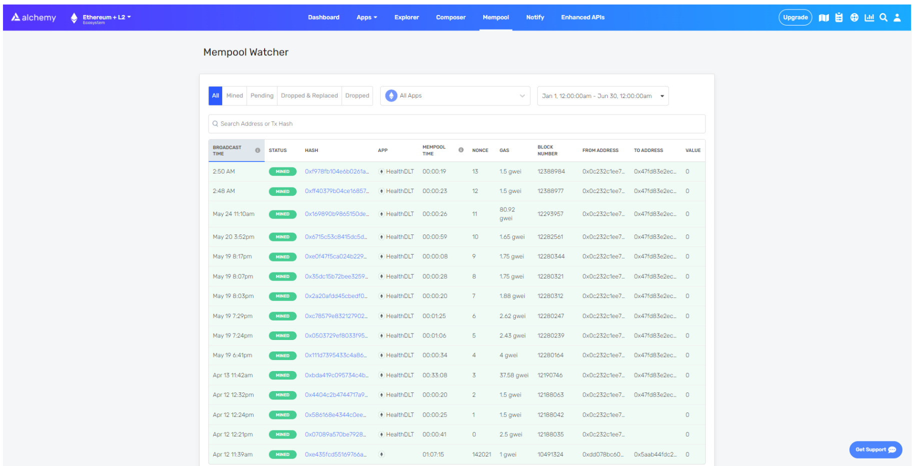
```
0: 0xf978fb104e6b0261afdb40f2ef29a3c8710cead47e30a32ec32a65ed53b0e9d6
```

```
Block Hash:             0xd6aee4c9ca0fc327a18b82e99be942f3ce3b9600cbd5ad2f6008fe404…
Block Number:           12388984
Contract Address:       null
Cumulative Gas Used:    1067470
Effective Gas Price:    1500000004
From:                   0x0c232c1ee719b9a6f0737d31f40d768228be4a2b
Gas Used:               29515
Logs:                   []
Logs Bloom:             0x0000000000000000000000000000000000000000000000000000000…
Status:                 0
To:                     0x47fd83e2ecf035acc45f7b9e1f3252a30ce1261d
Transaction Hash:       0xf978fb104e6b0261afdb40f2ef29a3c8710cead47e30a32ec32a65ed5…
Transaction Index:      20
Type:                   0
```

Figure 4.17: Alchemy Dashboard 2

One of the dashboards provided by Alchemy is called Alchemy Mempool (see figure 4.18), which provides information on the each individual transaction. Asides from being able to see what each transaction was for, it also provides valuable information on gas price, nonce, transaction time and addresses related to each individual transaction.

Like these services, there is also the possibility to check any transaction on Etherscan (see figure 4.19). Most public blockchains usually have a service like this attached to it to allow transparency on what transactions are happening throughout the network and to allow any user to track his own transactions, making it easier to detect any problems, anomalies or even to pinpoint where



Mempool Watcher

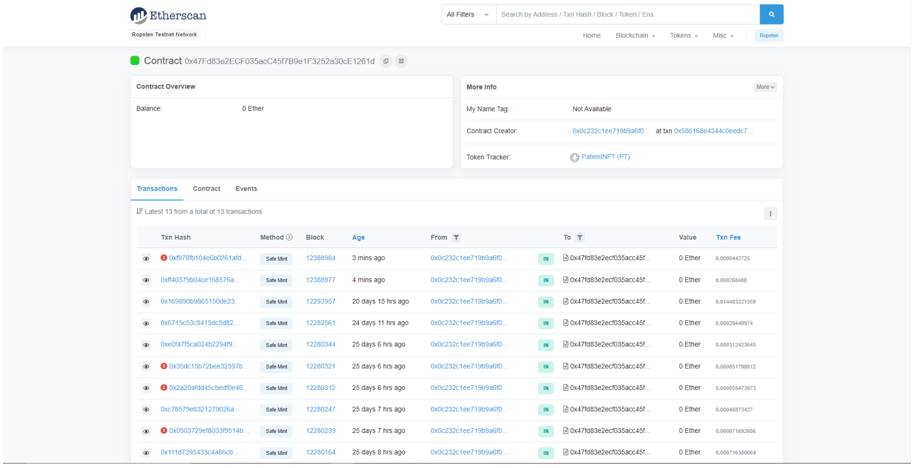
Jan 1, 12:00:00am - Jun 30, 12:00:00am

Search Address or Tx Hash

BROADCAST TIME	STATUS	HASH	APP	MEMPOOL TIME	NONCE	GAS	BLOCK NUMBER	FROM ADDRESS	TO ADDRESS	VALUE
2:50 AM	MINED	0xf978fb104e6b0261a...	HealthDLT	00:00:19	13	1.5 gwei	12388984	0x0c232c1ee7...	0x47fd83e2ec...	0
2:48 AM	MINED	0xff40379b04ce16857...	HealthDLT	00:00:23	12	1.5 gwei	12388977	0x0c232c1ee7...	0x47fd83e2ec...	0
May 24 11:10am	MINED	0x169890b9865150de...	HealthDLT	00:00:26	11	80.92 gwei	12293957	0x0c232c1ee7...	0x47fd83e2ec...	0
May 20 3:52pm	MINED	0x6715c53c8415dc5d...	HealthDLT	00:00:59	10	1.65 gwei	12282561	0x0c232c1ee7...	0x47fd83e2ec...	0
May 19 8:17pm	MINED	0xe0f47f5ca024b229...	HealthDLT	00:00:08	9	1.75 gwei	12280344	0x0c232c1ee7...	0x47fd83e2ec...	0
May 19 8:07pm	MINED	0x35dc15b72bee3259...	HealthDLT	00:00:28	8	1.75 gwei	12280321	0x0c232c1ee7...	0x47fd83e2ec...	0
May 19 8:03pm	MINED	0x2a20afdd45cbedf0...	HealthDLT	00:00:20	7	1.88 gwei	12280312	0x0c232c1ee7...	0x47fd83e2ec...	0
May 19 7:29pm	MINED	0xc78579e832127902...	HealthDLT	00:01:25	6	2.62 gwei	12280247	0x0c232c1ee7...	0x47fd83e2ec...	0
May 19 7:24pm	MINED	0x0503729ef8033f95...	HealthDLT	00:01:06	5	2.43 gwei	12280239	0x0c232c1ee7...	0x47fd83e2ec...	0
May 19 6:41pm	MINED	0x111d7395433c4a86...	HealthDLT	00:00:34	4	4 gwei	12280164	0x0c232c1ee7...	0x47fd83e2ec...	0
Apr 13 11:42am	MINED	0xbda419c095734c4b...	HealthDLT	00:33:08	3	37.58 gwei	12190746	0x0c232c1ee7...	0x47fd83e2ec...	0
Apr 12 12:32pm	MINED	0x4404c2b4744717a9...	HealthDLT	00:00:20	2	1.5 gwei	12188063	0x0c232c1ee7...	0x47fd83e2ec...	0
Apr 12 12:24pm	MINED	0x586168e4344c0ee...	HealthDLT	00:00:25	1	1.5 gwei	12188042	0x0c232c1ee7...		0
Apr 12 12:21pm	MINED	0x07089a570be7928...	HealthDLT	00:00:41	0	2.5 gwei	12188035	0x0c232c1ee7...		0
Apr 12 11:39am	MINED	0xe435fcd55169766a...		01:07:15	142021	1 gwei	10491324	0xdd078bc60...	0x5aab44fdc2...	0

Figure 4.18: Alchemy Mempool

the problem occurred when a transaction fails. Ethereum has Etherscan, and there is one for each network (mainnet or different testnets), which allows people to track these transactions not only on the main net but also on any test network. When using this website, one can check individual transactions, check addresses such as a patient's address or even a contract address, to see any incoming or outgoing transactions.



Contract 0x47Fd83e2ECF035acC45f7B9e1F3252a30cE1261d

Contract Overview

Balance: 0 Ether

More Info

My Name Tag: Not Available

Contract Creator: 0x0c232c1ee719b9a6f0... at txn 0x586168e4344c0eedc7...

Token Tracker: PatientNFT (PT)

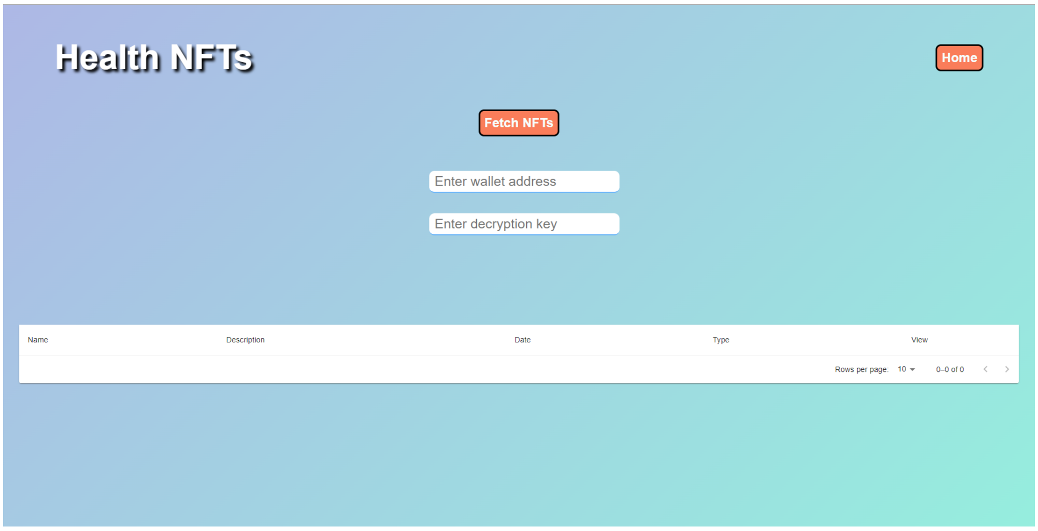
Latest 13 from a total of 13 transactions

Txn Hash	Method	Block	Age	From		To	Value	Txn Fee
❗ 0xf978fb104e6b0261afd...	Safe Mint	12388984	3 mins ago	0x0c232c1ee719b9a6f0...	IN	0x47fd83e2ecf035acc45f...	0 Ether	0.0000442725
0xff40379b04ce168576a...	Safe Mint	12388977	4 mins ago	0x0c232c1ee719b9a6f0...	IN	0x47fd83e2ecf035acc45f...	0 Ether	0.000268488
0x169890b9865150de23...	Safe Mint	12293957	20 days 15 hrs ago	0x0c232c1ee719b9a6f0...	IN	0x47fd83e2ecf035acc45f...	0 Ether	0.014483221359
0x6715c53c8415dc5d82...	Safe Mint	12282561	24 days 11 hrs ago	0x0c232c1ee719b9a6f0...	IN	0x47fd83e2ecf035acc45f...	0 Ether	0.00029449974
0xe0f47f5ca024b2294f9...	Safe Mint	12280344	25 days 6 hrs ago	0x0c232c1ee719b9a6f0...	IN	0x47fd83e2ecf035acc45f...	0 Ether	0.000312423045
❗ 0x35dc15b72bee32597b...	Safe Mint	12280321	25 days 6 hrs ago	0x0c232c1ee719b9a6f0...	IN	0x47fd83e2ecf035acc45f...	0 Ether	0.000051798812
❗ 0x2a20afdd45cbedf0e46...	Safe Mint	12280312	25 days 6 hrs ago	0x0c232c1ee719b9a6f0...	IN	0x47fd83e2ecf035acc45f...	0 Ether	0.000055473973
0xc78579e8321279026a...	Safe Mint	12280247	25 days 7 hrs ago	0x0c232c1ee719b9a6f0...	IN	0x47fd83e2ecf035acc45f...	0 Ether	0.00046873427
❗ 0x0503729ef8033f9514b...	Safe Mint	12280239	25 days 7 hrs ago	0x0c232c1ee719b9a6f0...	IN	0x47fd83e2ecf035acc45f...	0 Ether	0.000071692606
0x111d7395433c4a86cb...	Safe Mint	12280164	25 days 8 hrs ago	0x0c232c1ee719b9a6f0...	IN	0x47fd83e2ecf035acc45f...	0 Ether	0.000716380664

Figure 4.19: Ropsten Etherscan

4.5.2 List NFTs

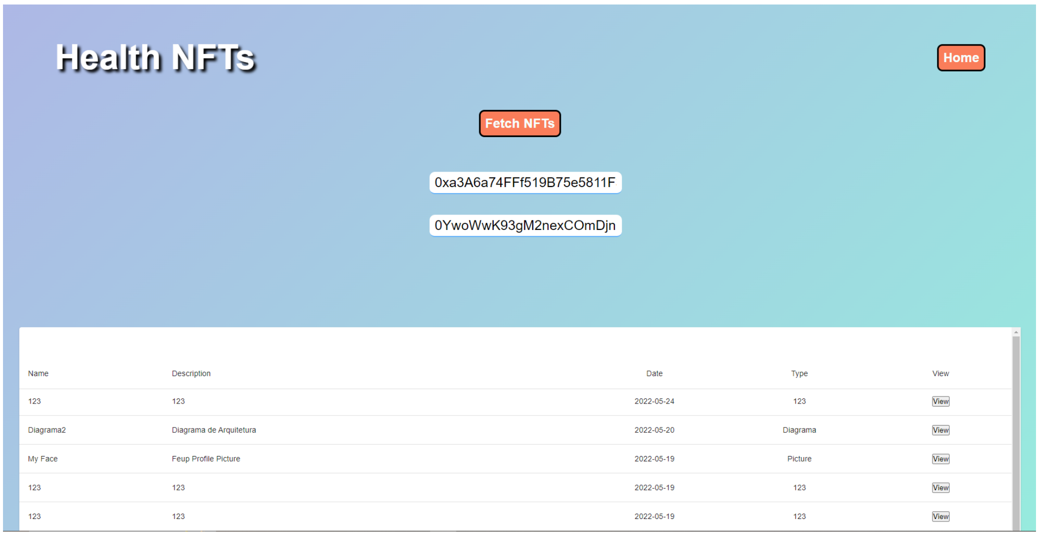
The listing part of the app is available regardless of authentication as it is the part of the app that the common patient would use on their own to check the healthcare data stored on his wallet at any given moment. It could also be used by a doctor or another health professional during consultation to help check certain information that might aid in the moment if the patient provides him with his information. When clicking on the button in the home page, the user is redirected to another small form which has only 2 fields (see figure 4.20), patient address and encryption key, which will be used to decrypt the files stored in the NFTs.



Name	Description	Date	Type	View

Rows per page: 10 ▾ 0–0 of 0 ‹ ›

Figure 4.20: List form screen



0xa3A6a74FFf519B75e5811F

0YwoWwK93gM2nexCOmDjn

Name	Description	Date	Type	View
123	123	2022-05-24	123	View
Diagrama2	Diagrama de Arquitetura	2022-05-20	Diagrama	View
My Face	Feup Profile Picture	2022-05-19	Picture	View
123	123	2022-05-19	123	View
123	123	2022-05-19	123	View

Figure 4.21: Listing NFT screen

When submitting the form, the Moralis API uses the provided address and fetches all the NFTs belonging to that address in the specified chain, in this case, the Ropsten Ethereum Testnet. After this, it forwards all of the NFTs and the encryption key provided to the back end of the prototype system, where the files are downloaded, decrypted using the provided key and then forwarded to the front end of the app, where they'll be available to be displayed. When submitting the form on the listing page, there is a table which will be filled with the files that come as a response from the backend (see figure 4.21). The table contains columns for all the information, the name, description, date, type of file and then the view column. This last column is essentially full of buttons in every row, each button will redirect the user to a page with the corresponding file resource displayed on it.

4.6 Chapter Summary

In this chapter, we introduced individually the technologies used and chained when developing the prototype, provided in-depth information of what each of them brought to the prototype and potential downsides. We also described what was done and how the technologies were integrated into the prototype.

Chapter 5

Experimentation and Results

This chapter presents the experimentation that was performed over the developed prototype. The previous chapter described this prototype which, as described, encompasses a proof of concept towards the technological requirements for storing and accessing medical data through NFTs and blockchain. The current chapter presents results that were achieved and how that reflects the success or failure of this solution.

Starting with section 5.1, which goes over the description of the use case in question and how that use case would be evaluated, a description of the prototype and its purpose and an experiment setup going over preconditions and requisites for this prototype. Following that, section 5.2 presents the structure of what a test would be like and how long it would take, as well as what tasks would have to be performed during it, what would constitute success and failure and finally the experiment's metrics. Section 5.3 presents a timeline of the order of implementation of the prototype's features and how testing affected the decisions during the research of the solution and the corresponding prototype development. Section 5.4 outlines the strengths and weaknesses of this solution based on the previously shown information. Finally section 5.5 presents a summary of this chapter contents.

5.1 Experimentation Design

5.1.1 Experiment Description

The experiment consists of a scenario in which:

- The patient attends a appointment on a medical facility that has access to the developed dApp.
- During registration at the health care facility, the patient provides his wallet address and public key at the reception which gets inserted into the system. This data is then used during the appointment by the doctor (in a transparent manner) to access existing medical data. The accessible contents consists in a table containing all previously acquired medical documents that have been submitted and minted into NFTs.

- This allows the doctor to search for any diagnostically relevant documents belonging to that patient. After the appointment, any documents and diagnostics resulting from it can be uploaded into the app and then minted into NFTs which becomes available in the patient medical record. This is achieved by someone in the healthcare facility submitting the data into the Uploading part of the dApp, along with details about the document such as date, type of document, name and description and specifying the patient's address where the documents are stored and the public key that is used to encrypt the uploaded file. After the upload of the files, they become available in the listing part of the app in approximately 30 minutes and can then be seen by the patient as well if they enter their address and public key on the app by themselves, at home or anywhere else.
- In a production system much of the given details can be transparent to the users because the IT applications can perform these tasks. One important perspective remains that consists of the legal perspective and of the fact that entities may be legally obliged to "forget" public keys after the medical acts are completed of after a defined time period.
- In case the patient is new and has never used this type of technology, it can simply create an address in any of the possible options (metamask, coinbase or phantom) and then, by the doctor uploading the files to that address without specifying a public key, one is automatically generated and provided to the doctor, who can then give it to the patient to keep and use futurely.

5.1.2 Prototype Description

The prototype intends to shift the control of information from the medical institutions to the patient itself, but since this depends on other external factors such as regulation, as a main function, it intends for people to be able to carry their own medical information wherever they go in the world, facilitating diagnosis for people who travel or even start living somewhere else different, which might not normally have access to the previously obtained medical files. Furthermore, from a medical record point of view, patients get their independence from any particular health care insurance, protection system or private facility.

The prototype takes a file uploaded by the medical staff along with the information that was input alongside it, encrypts it, stores them as files in a decentralized storage, the Inter Planetary File System (IPFS) by means of the Pinata API and then provides the URI of the metadata for the smart contract to mint into an NFT, which is automatically sent to the address provided (see figure 4.8). This connection to the chain is attained thanks to the Alchemy servers which facilitate the use of networks such as Ethereum or Polygon. There is also an option which allows people to input an address and a public key for the app to fetch, decrypt and then list all of the NFTs that belong to that address (see figure 4.9). With the help of the Moralis API, it is possible to fetch all this information from any supported chain, which is then sent to the app and decrypted with the provided key and then displayed on the screen for the user to access/see or even potentially burn the token in case of any error.

5.1.3 Experiment Setup

For this app to be used, the requirements would be for the medical facility in question to have access to this app and to possess an administrator account and for the user to possess a wallet address. These could be of any sorts, metamask, phantom, coinbase. The is no need for a user to have a public key as the app will generate one for the user in case they have not provided one yet. It is however important that the provided key pair is kept by the user and used in further appointments as it should be the same for all the files. If not, the decryption process will then have problems. As in other identification systems, a card containing a programable chip could be become a solution to store the keypair.

Technology is usually the barrier that stops many less knowledgeable people from using very useful resources which are commonly available to society. People are afraid of what's new and what they cannot understand and this may seem a possible scenario when addressing blockchain and NFTs. There is also the need to be wary to scams and other malicious appliances that these technologies pose. As an example of scams, one can mention multiple kinds of credit card or even bank app scams which have surfaced in the past few years. People convincing usually older people to go to an ATM and select certain options which end up giving the scammer access to the victim's bank account or something similar.

These types of situations highlight the dangers of technology when it's used in fields of sensitive information and therefore give a reason for people to be instructed on these subjects before using them for their own benefit. Both health workers and patients adhering to this type of technologies should be instructed and made aware of how to navigate them and what dangers may arise from an inadequate use of them.

5.2 Features and Metrics

5.2.1 Methodology

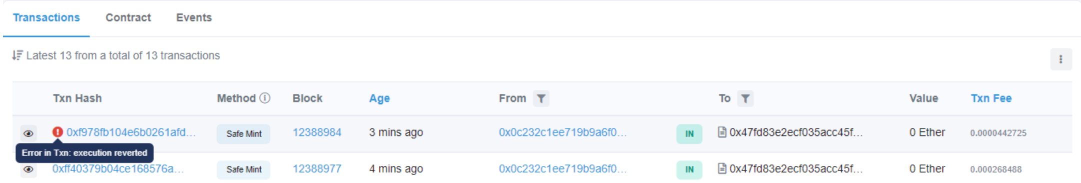
To test the app, one can input a file and information alongside it, providing an address and key. To then verify if the file has successfully been minted into an NFT, we can check the same address and see if the file shows up. For the time it takes, luckily, Alchemy provides a feature, Alchemy mempool, which provides information on the transactions performed by the app such as exact gas fee and time it took to be accepted. This allows us to monitor how long each individual transaction took, estimate a time for it and even explore any outliers that may pop up. There is also the possibility to check the status on Etherscan which usually shows status of the transaction at a given moment. Unfortunately, despite a transaction being completed, the NFT does take some time to show up when fetching information with the Moralis API. Presumably this wait time arises from every NFT taking around 30 minutes to show up in its respective wallet. It may be a limitation or configuration of the enabling technology.

Due to this being a proof of concept and an attempt at chaining technologies in efforts of creating a possible solution, stress testing the prototype would not produce any relevant results as they wouldn’t be comparable to the currently used systems, and therefore, have no real meaning. Since this prototype provides more of a proof of concept on the integration of these technologies for the specific topic of health data, it is expected that multiple parts of the process are slower than they could eventually be due to lack of optimization, which would render batch testing sort of pointless. Opposed to that, the test is more focused on the fact that the information is being encrypted with the correct key uploaded to the decentralized storage, minted into an NFT and sent to the provided address, making it available soon after the service provider or any patient clicks the submit button. There are also possibilities of testing what would happen if the credentials given are not valid or do not align to what was previously provided.

5.2.2 Performed Tasks

The condition for success is to be able to fetch the uploaded files and display them on screen when requested, meaning that these have been turned into NFTs successfully and are now available for the patient anywhere he goes, as long as he has access to his address and public key. There is also the case of submitting a wrong key by mistake or by any malicious user, which results in "broken files" which cannot be displayed on screen due to a failure in the decryption process, as the key is wrong.

There is yet another specific condition of failure for this app which is a transaction that, according to Alchemy mempool has been completed, but returns a message of "transaction reverted" (see figures 5.1 and 5.2).

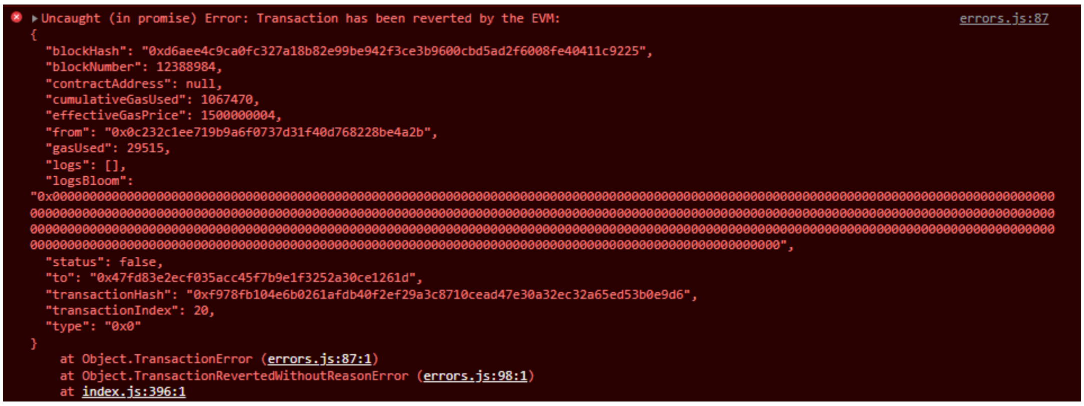


Latest 13 from a total of 13 transactions

Txn Hash	Method	Block	Age	From		To	Value	Txn Fee
0xf978fb104e6b0261afd...	Safe Mint	12388984	3 mins ago	0x0c232c1ee719b9a6f0...	IN	0x47fd83e2ecf035acc45f...	0 Ether	0.0000442725
0xff40379b04ce168576a...	Safe Mint	12388977	4 mins ago	0x0c232c1ee719b9a6f0...	IN	0x47fd83e2ecf035acc45f...	0 Ether	0.000268488

Error in Txn: execution reverted

Figure 5.1: Reverted Transaction on Etherscan



```
▸Uncaught (in promise) Error: Transaction has been reverted by the EVM:                errors.js:87
{
  "blockHash": "0xd6aee4c9ca0fc327a18b82e99be942f3ce3b9600cbd5ad2f6008fe40411c9225",
  "blockNumber": 12388984,
  "contractAddress": null,
  "cumulativeGasUsed": 1067470,
  "effectiveGasPrice": 1500000004,
  "from": "0x0c232c1ee719b9a6f0737d31f40d768228be4a2b",
  "gasUsed": 29515,
  "logs": [],
  "logsBloom":
"0x000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000",
  "status": false,
  "to": "0x47fd83e2ecf035acc45f7b9e1f3252a30ce1261d",
  "transactionHash": "0xf978fb104e6b0261afdb40f2ef29a3c8710cead47e30a32ec32a65ed53b0e9d6",
  "transactionIndex": 20,
  "type": "0x0"
}
    at Object.TransactionError (errors.js:87:1)
    at Object.TransactionRevertedWithoutReasonError (errors.js:98:1)
    at index.js:396:1
```

Figure 5.2: Reverted Transaction on the Console

Despite the trials, there was an inability to reproduce this specific problem with any consistency as it seems to be either random or dependant on network status, therefore, despite the validation of the transaction, the NFT with the corresponding medical file is never created and therefore never fetchable. A system facing this error could acknowledge the situation display the specific error as a message for the medical staff in order to warn and attempt to resubmit the request.

5.3 Tests

This section focuses on the two distinct testing phases which existed during the development of the solution and the corresponding prototype. A first version, more exploratory was developed with the intent to assess and test out multiple possible technologies and evaluate which would work better for the intended purpose. A second and final version including the full prototype that would allow the users to mint NFTs, to access them and to be able to view their resources.

5.3.1 First Prototype

When approaching the technologies for the first time, the goal, rather than trying to make the application work immediately, was to study and try out different approaches and then check compatibility between the development of each smaller step such as the front-end, the back-end, the specific integration with each individual technology and figuring out how to make all of them work together. Since the base scenario was to make NFTs out of patient's health data, the initial approached was more based on learning about NFTs themselves and the smart contract that would act as a bridge between the app and the network. Therefore, for the initial prototype, the app would basically be comprised of only the uploader that was mentioned in section 4.5.1, but not including the encryption of the files as this would make it harder to test if the NFTs were being properly minted and reduce the utility of the Pinata API mentioned in section 4.2. This API offered visibility on the files that were being uploaded and feedback on if they had been properly uploaded and if the URIs that were put on the NFTs were correct or not. Since there was no way of listing NFTs yet, the whole process of encrypting and decrypting files would add an unnecessary layer of complexity to the early testing and make it harder to test out the interaction between the technologies that were being used and implemented at the time.

This first solution would allow health workers to turn any medical exam into an NFT and forward it to the corresponding patient's address in a scenario where the payment of gas is handled by the health facility in question. This helps take the first step towards saving information as NFTs, allowing people to carry it around and show it when necessary and proving that this information belongs to them, as it is displayed in an NFT, bound by the signature of a digital smart contract.

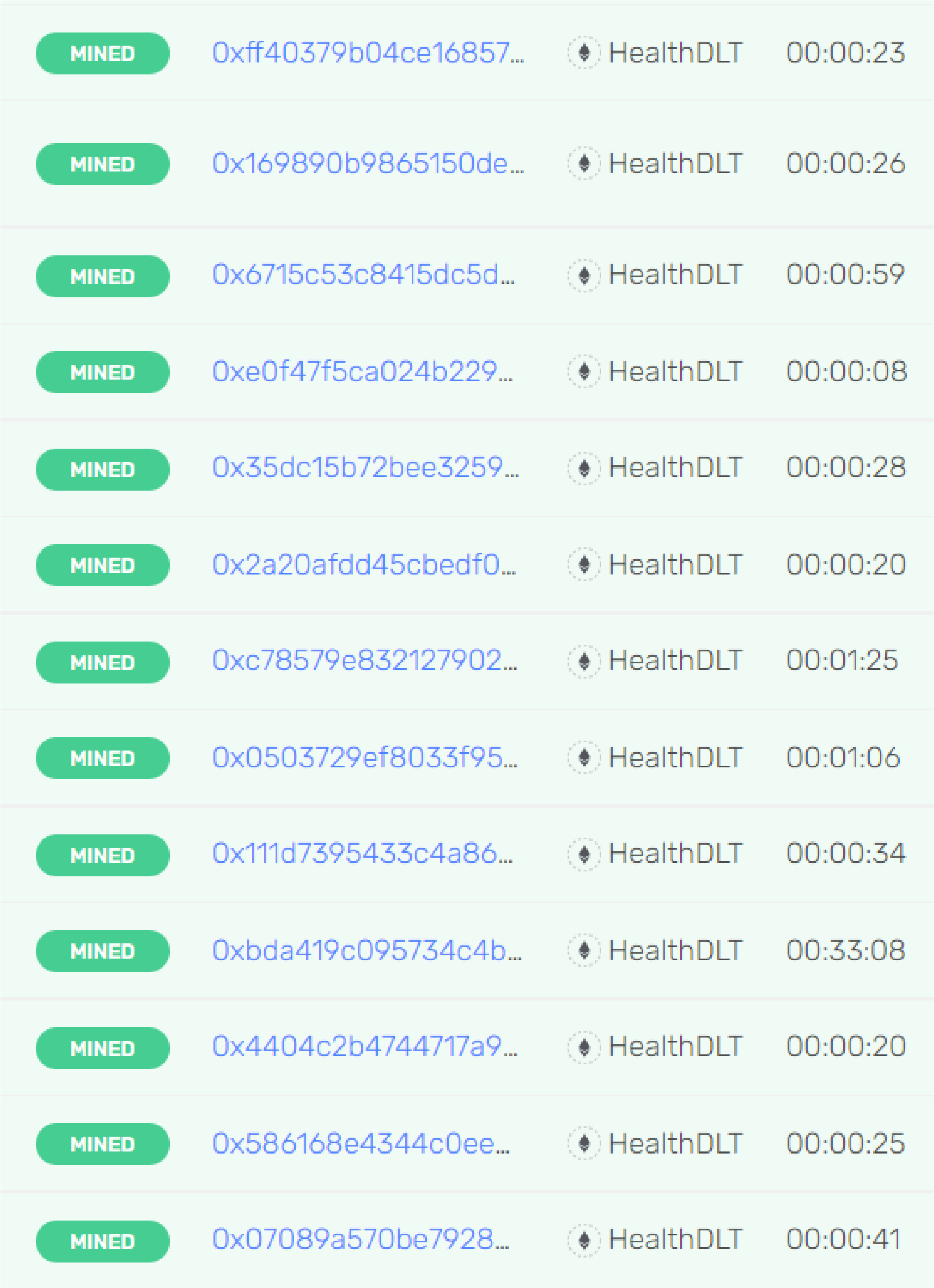
The first solution presented some problems which impact viability of the prototype and were important to be addressed.

The biggest and most obvious one is the fact that this version was based and supported on public services and tools which are available online, but are in fact dependant on other institutions and the services provided by them. This also means that most of the information is public as well, considering there are no encryption algorithms being used on the information before uploading it into the storage and the chain. This makes all the information that is uploaded completely public and accessible by anyone who is in possession of the patient's wallet address, which is not private information. Especially considering the specific use case in question is regarding health data, this is a deal breaker and something that would easily make the whole concept unviable for this use case.

There were also noticeable problems when looking into the Alchemy Mempool (see figure 5.3), which show certain transactions taking 30 seconds, but others taking comparatively much greater amounts of time, such as 30 minutes, which makes the whole process less reliable and less consistent.

Although the public platforms do have private options, which are mostly payed options, most of these services could be implemented in the future and integrated as a part of the current product turning the prototype into the whole package and making everything depend solely on how things are handled within the same organization and facilitating development. Having all of these tools within the same ecosystem, although raising centralization of the services, could also improve the compatibility between the individual parts of the system which could result in an increase in availability and optimization of the whole process. As it would be giving more power and control to one single organization this could bring forward the concern of centralization, but would come as a trade-off regarding the efficacy of the product.

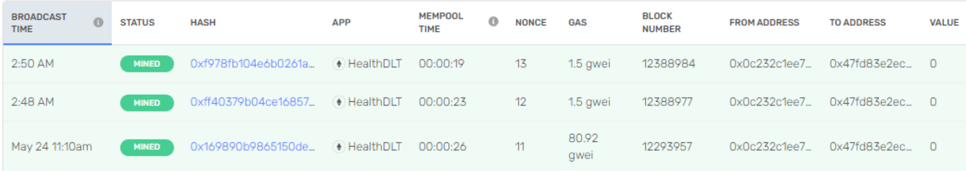
Considering the fact that the information is public, a solution involving encryption was considered. As there are no blockchain encryption feature for data inside the each block, the considered solution was to encrypt data before uploading to IPFS and then decryption as the NFTs contents are fetched, before displaying them, making it so that despite the platforms can be public, the information that is displayed is actually not valid, as it is encrypted and therefore not viewable. Considering the most known algorithms and proper encryption techniques, there is usually a public and/or a private key in the mix, when these algorithms are concerned. Methods such as AES, which is commonly known requires a public key for encryption and decryption. The concern with using these methods is whether the prototype would contain a database with the keys or whether the user would be granted full control, being given to him a key which he would have to present every time he wished to use the app or presented himself to a health appointment. Although this would give patients one more weird code to carry with them, it would increase the control the user has on his own information and reduce the need for a database associated with the system. This database would also take back some of the utility of a distributed solution as the healthcare facilites would have access to patient information due to keeping database keysets which would pose a point of failure and vulnerability. There is however the concern that people might lose or give the key to someone they should not which also poses a security threat to them. Besides that, the common person would not be used to just carrying around 2 codes (address and public key) that they would present when going to a healthcare facility. People are used to presenting information from their ID Cards for example, which could be an add-on that would facilitate the whole process for the general public.



MINED	0xff40379b04ce16857...	HealthDLT	00:00:23
MINED	0x169890b9865150de...	HealthDLT	00:00:26
MINED	0x6715c53c8415dc5d...	HealthDLT	00:00:59
MINED	0xe0f47f5ca024b229...	HealthDLT	00:00:08
MINED	0x35dc15b72bee3259...	HealthDLT	00:00:28
MINED	0x2a20afdd45cbedf0...	HealthDLT	00:00:20
MINED	0xc78579e832127902...	HealthDLT	00:01:25
MINED	0x0503729ef8033f95...	HealthDLT	00:01:06
MINED	0x111d7395433c4a86...	HealthDLT	00:00:34
MINED	0xbda419c095734c4b...	HealthDLT	00:33:08
MINED	0x4404c2b4744717a9...	HealthDLT	00:00:20
MINED	0x586168e4344c0ee...	HealthDLT	00:00:25
MINED	0x07089a570be7928...	HealthDLT	00:00:41

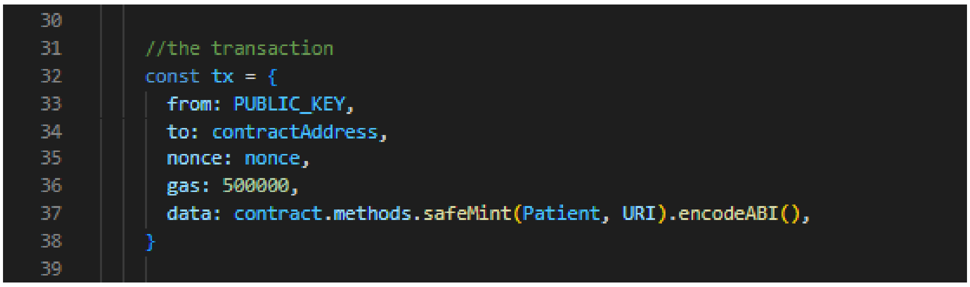
Figure 5.3: Sample of Transaction Times

Concerning the big discrepancies noticed between different transactions (see figures 5.4 and 5.5) when their duration is taken into account, after some research, it was found that when the network is overloaded or, put simply, has a lot of transaction requests coming through, these transactions are ordered and filtered not by the order in which they come in or are made, but by the gas that each person is willing to pay as a fee for that transaction. This means that paying higher gas fees also means transactions will have priority over other transactions in which the users decided to pay less fees.



BROADCAST TIME	STATUS	HASH	APP	MEMPOOL TIME	NONCE	GAS	BLOCK NUMBER	FROM ADDRESS	TO ADDRESS	VALUE
2:50 AM	MINED	0xf978fb104e6b0261a...	HealthDLT	00:00:19	13	1.5 gwei	12388984	0x0c232c1ee7...	0x47fd83e2ec...	0
2:48 AM	MINED	0xff40379b04ce16857...	HealthDLT	00:00:23	12	1.5 gwei	12388977	0x0c232c1ee7...	0x47fd83e2ec...	0
May 24 11:10am	MINED	0x169890b9865150de...	HealthDLT	00:00:26	11	80.92 gwei	12293957	0x0c232c1ee7...	0x47fd83e2ec...	0

Figure 5.4: Difference noticed in Gas Fees of different transactions



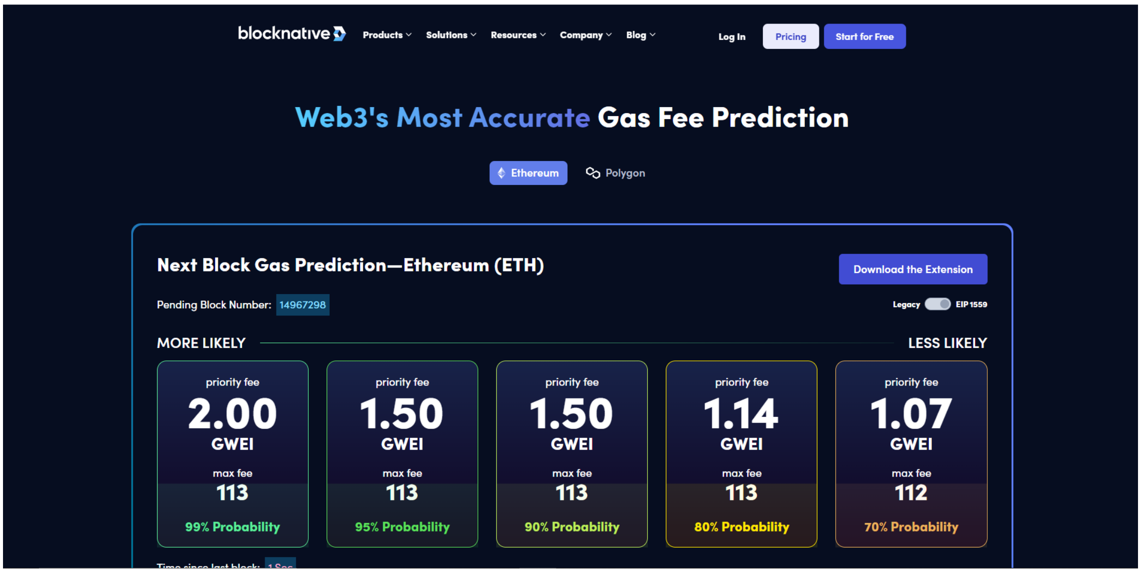
```
//the transaction
const tx = {
  from: PUBLIC_KEY,
  to: contractAddress,
  nonce: nonce,
  gas: 500000,
  data: contract.methods.safeMint(Patient, URI).encodeABI(),
}

```

Figure 5.5: Code snippet defining max transaction gas (Gwei)

Gas fees can seem like a hard concept to grasp, in fact it is like the tax that people pay at any service they use or take advantage off. These are essentially costs that help maintaining the chain and that every transaction requires. They can vary however depending on the type of transaction or even on the current state of the network when making these transactions. These are usually measured in either Ether or Gwei, Ether being the currency used in the Ethereum network and Gwei being a smaller portion currency which was designed specifically for these smaller costs as it represents 10^{-9} ether, which means there are 1 Billion Gwei in an Ether (ETH).

Considering the particular use case, there is usually no rush for the user to get their NFTs minted, but depending on the situation, there could be an option to help accelerate the file submission process in case of necessity or urgency. There is also the option of integrating a system which could detect the state of the network and calculate gas depending on it such as Block Native (see figure 5.6), Gwei.at (see figure 5.7) and Eth Gas Station (see figure 5.8), which are online services that already help track these metrics and serve as a reference for people who are making their own transactions, helping them opt for the cheapest possible gas fee available.

BlockNative.com



Web3's Most Accurate Gas Fee Prediction

Next Block Gas Prediction—Ethereum (ETH)

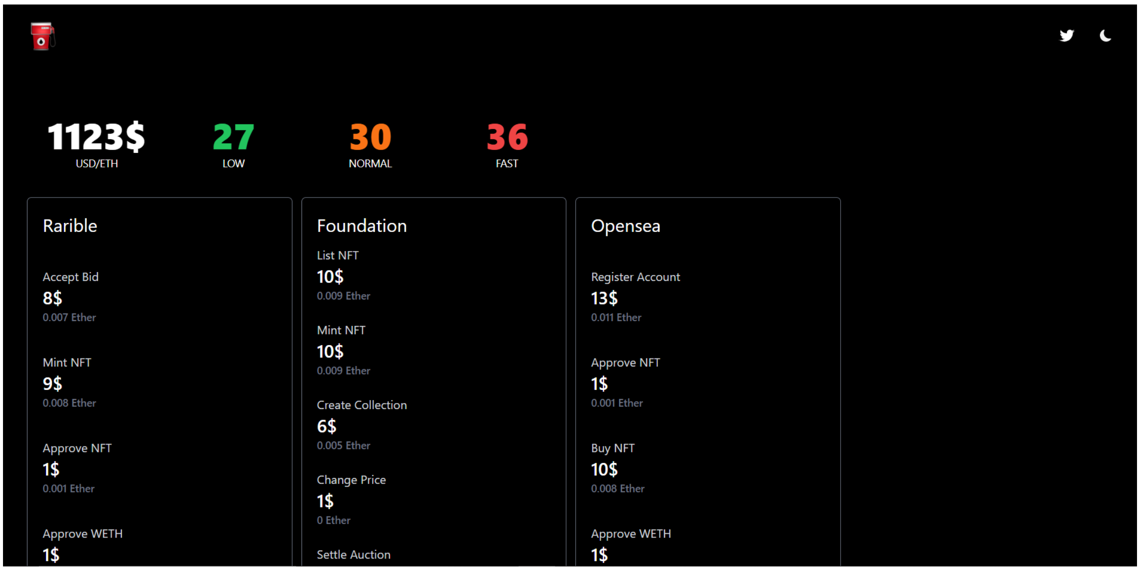
Pending Block Number: 14967298

MORE LIKELY				LESS LIKELY
priority fee 2.00 GWEI	priority fee 1.50 GWEI	priority fee 1.50 GWEI	priority fee 1.14 GWEI	priority fee 1.07 GWEI
max fee 113	max fee 113	max fee 113	max fee 113	max fee 112
99% Probability	95% Probability	90% Probability	80% Probability	70% Probability

Time since last block: 1 Sec

Figure 5.6: BlockNative.com

Gwei.at



1123$	27	30	36
USD/ETH	LOW	NORMAL	FAST

Rarible

Accept Bid
8$
0.007 Ether

Mint NFT
9$
0.008 Ether

Approve NFT
1$
0.001 Ether

Approve WETH
1$

Foundation

List NFT
10$
0.009 Ether

Mint NFT
10$
0.009 Ether

Create Collection
6$
0.005 Ether

Change Price
1$
0 Ether

Settle Auction

Opensea

Register Account
13$
0.011 Ether

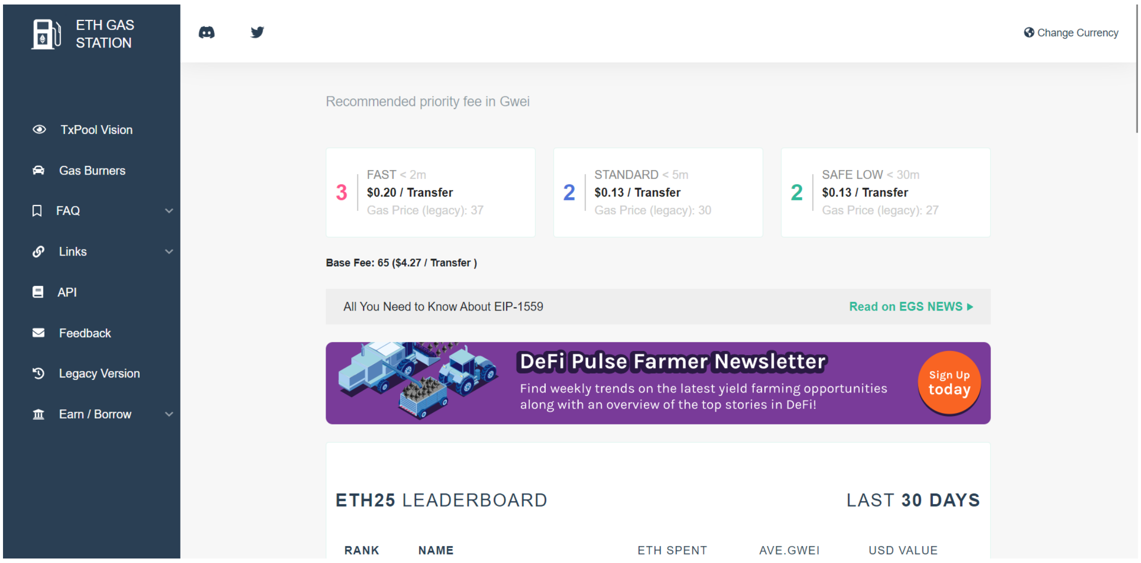
Approve NFT
1$
0.001 Ether

Buy NFT
10$
0.008 Ether

Approve WETH
1$

Figure 5.7: Gwei.at

Ethgasstation.info



Recommended priority fee in Gwei

3 FAST < 2m
$0.20 / Transfer
Gas Price (legacy): 37

2 STANDARD < 5m
$0.13 / Transfer
Gas Price (legacy): 30

2 SAFE LOW < 30m
$0.13 / Transfer
Gas Price (legacy): 27

Base Fee: 65 ($4.27 / Transfer)

All You Need to Know About EIP-1559

DeFi Pulse Farmer Newsletter
Find weekly trends on the latest yield farming opportunities along with an overview of the top stories in DeFi!

ETH25 LEADERBOARD LAST 30 DAYS

RANK	NAME	ETH SPENT	AVE.GWEI	USD VALUE

Figure 5.8: Eth Gas Station

Due to this being out of scope, it will not be implemented in this specific prototype, but it is a viable option when regarding gas prices for transactions, given that the information is all public and could be fetched via Etherscan, making it possible to estimate average gas prices in the latest transactions and applying that gas price to the specific transaction in question.

5.3.2 Final version of the prototype

Considering the problems still existing in the initial prototype, and after considering how much effort each of these would take, some were chosen and developed upon, to attain a prototype which would cover as many aspects as possible in the time available for development.

During the improvement of the initial prototype, it made sense to have a way to see the NFTs on the app as well, that way, patients would be able to not only show their medical information during a health appointment, but would also be able to see their own results at home to check if anything was wrong following their previous trip to a health establishment. Therefore, a listing app was created and joined to the original prototype. That way, the app could handle both sides of the use case, the creation of the NFTs with the health data and the view of those NFTs whenever required by the patient, without them having to resort to other applications.

Since both the upload and the listing of the NFTs were now a part of the prototype, encryption was the next feature to be added to it, since the prototype would be responsible for the information before the NFT was made and before the information was listed on screen. Therefore, the AES encryption algorithm was used on the back-end of the application, using the key that was in possession of the patient in order to encrypt when uploading and decrypt when listing.

The fact that the files are encrypted now gets rid of a significant security problem that was present in the first prototype because the information was public and visible to anyone with knowledge of the patient's address, making it a poor solution for the storage of health data. Previously, all the file contents could be seen just by opening their URI and even just by going to the Pinata dashboard, any file uploaded there would have been visible.

In the implementation of the encryption feature, to reduce the need for a database, the keys are automatically generated in case one is not provided during upload (for new patients), but already existing patients, should provide their original key as that is the key they will provide in order to decrypt the information later on. Although this gives room for human error when providing the keys and can lead to slight setbacks, it seemed better than the healthcare facilities possessing a list of keys and addresses from the patients, which would essentially grant them the ability to view information at any time, taking a portion of the value of this prototype away.

5.3.2.1 Existing Problems

Considering the problems mentioned in the previous prototype and the ones that were solved when developing the final prototype, the remaining problems persist. There has not been a change in technologies from one prototype to the other, meaning that this final product is still based on public platforms which belong to other organizations and are therefore out of our control. If any of these is changed and or removed, there will be the need to change the prototype as well or even the need to find another technology which can replace the previous one's functions.

There is also the fact that the gas fees being currently applied are not being dinamically adjusted to the current state of the network, so, even though the amount might be slightly higher than in the first prototype, to reduce errors during testing and unusually long transactions, there is no guarantee the currently specified amount will be useful in busy periods of the network or that it will be appropriate for periods of low activity as well.

Aside from that, despite the creation of NFTs with health data, there is nothing in the prototype that prevents health facilities from keeping the information in their systems after uploading it to the patient's wallet. This could only be controlled by complementing this program with the adequate legislation which would prevent healthcare institutions and workers from keeping and sharing medical details. As such thing is out of scope for this project, it will focus more heavily on providing the patient more control and access to its own information, instead of reducing the control that other institutions have on the that was obtained in their facilities.

5.4 Results and Discussion

5.4.1 Benefits

Regarding the overall prototype and use case scenarios developed, this is a strong option for people who need to travel a lot or who go to different medical facilities often. Assuming that some derivation of this prototype would be picked up by organizations, this would allow people to have their medical information available to them at all times as long as they had access to the website/app, be it to check the results of their latest medical exams or to show them to any health professional they deem appropriate that might need the information for diagnosis or even for medical advice (something that would be the patient's option as it is their health data). The prototype is based on the second biggest blockchain currently available as well as being able to be switched into a smaller, cheaper but also very known network due to compatibility between them and therefore has plenty of documentation that could help not only maintain but also develop this approach further. Considering that this technology is fairly recent and that most use cases for NFTs are still based on digital art, there is still plenty to be explored and it is likely that the technology of NFTs and blockchain in general will be explored further, creating new approaches which might in the future prove valuable to the use case explored in this prototype.

5.4.2 Weaknesses

Despite the upsides of this prototype and what it might bring to various fields like healthcare or any other sort of information storage scenario, there are also downsides, not only comparing to what the prototype was expected to do at first, but also in general, as a technology that may come to be used in the future.

When regarding the shift of control of information from the hospitals to the patient, it is hard to tell how well this specific concept would do. There is a lot of legislation and other obstacles to this technology which are not related to this area of technical work and therefore are not covered by this prototype. There is an inability to prevent hospitals or individual health workers from downloading files, storing public keys and addresses to check patient information later or even just keep the copies of files they upload using the app. What this means is that there is no way, from the development and testing of this prototype to prevent other entities from keeping the patient's data and or sharing it in any way, as this would have to come from other areas, not just the technical one.

The display of the files is currently made to support images, but it is uncertain about other types of files due to inconsistency when trying to show them on screen, therefore, there would be the need to, in an initial stage, upload image versions of possible PDFs or whatever file would be produced during the health appointment to consistently use the product without adding more obstacles.

As a technology regarding health, it is safe to assume that this is targeting the general public and all types of people, meaning that a good part of the people using such a system would be older or perhaps not as technology savvy. This means there should be some sort of guide that should be provided for them, not only in how to utilize this prototype but also how to NOT utilize it in order to prevent any malicious actions from 3rd parties. It is a common occurrence that people will seek less knowledgeable people in predatory ways to trick them into doing certain things with these technologies which may cause great harm and stress to the targeted individuals. Even on the other side of things, using a prototype like this would also expose the staff at healthcare facilities to these technologies, meaning these would most likely also need to be educated on these matters and made aware of what can and cannot be done with a prototype like this, not only for them to make better use of it, but also to help clarify any issues that might come up from the patients.

5.5 Chapter Summary

In this chapter we presented in more detail the test scenarios, how to evaluate them based on the prototype that was implemented and then discussed a bit about the benefits and weaknesses of that same prototype according to the information that was retrieved. In section 5.2.2 it was also mentioned what would constitute success and failure and highlighted a specific and crucial error that occurred during the testing phase.

Chapter 6

Conclusions

This chapter presents this dissertation's conclusions. Section 6.1 describes the findings and the steps taken in the implementation, testing and results. Finally, section 6.2 details aspects with potential value following this dissertation and the prototype that was implemented during it.

6.1 Conclusions

To conclude this work, the prototype that was developed was a mostly successful implementation of what had been theorised previously. The whole dissertation serves as a proof-of-concept that with some time and the correct optimizations, the technologies of Blockchain and NFT can indeed be used for the storage of important information and then be carried by the user wherever it is needed.

The prototype itself shows how the files themselves can be turned into encrypted NFTs which are not visible by anyone except the patient who is in possession of the correct credentials to fetch and decrypt the information stored in those tokens. Despite the reported weaknesses in the prototype but also considering that these technologies currently possess close to no use cases aside from the digital art, there is a possibility for the extension of NFTs to not only healthcare but also many other areas which may require proof of ownership and authenticity of information.

Regarding the problem refered in Section 1.2, the obtained solution can indeed act as a way of storing information in a secure way due to the encryption of the files and then act as a personal patient file which we can access using the prototype that was developed. There is however the other part of the problem, shifting the control from healthcare organizations into the patient. This part is not solved using this prototype and is part of the future works as it involves other areas such as the legislation surrounding the storage and disclosure of information. In Section 1.3 it is hypothesised whether or not NFT and blockchain can be used to secure patient's sensitive and relevant health information, granting the patient proof of ownership over this information, and allowing the user to share this data with healthcare facilities when needed and for as long as needed. It has been concluded that NFTs can in fact act as viable ways to store the information and allow the user to carry it as a portable medical history. Due to the nature of the technology, the NFT grants proof of ownership and authenticity of the data. The prototype grants a way of accessing that information and sharing it when needed with the appropriate entities. Considering the goals set for the dissertation during Section 1.4, it is safe to say that most of them were met and that implementation and development went as expected. The prototype does essencially what was thought out for it to do and the extra research allowed to detect potential limitations and extra features that could be implemented in future works in order to complement what has already been done.

6.2 Future Work

Considering that this work is based on relatively new technologies of Blockchain and NFT and that, for the latter, most use cases available are directed towards digital art, there is a considerable amount of progress that can be made in following years based on them. Given the research and work done during implementation, some aspects that could be developed upon, to push this prototype further are:

- **The Burn Method** - Which was developed in the smart contract but it is not working in the prototype due to errors when logging in and requesting the transaction.

- **Optimizations In Interactions** - Improvements on the interactions between the tools to reduce delays during the usage of the prototype, as well as improvements in front-end and back-end to make the whole user experience flow better.

- **Extending File Format Displays** - The current prototype loads the files as images, so the file format is reduced to image formats. Implement adaptability that will support multiple file types such as PDFs or even videos.

- **Way of Carrying the patient Address and Encryption Key** - The address and encryption key are usually codes with a large amount of characters that are hard to tell someone else. Therefore the use of a card such as our ID card that would hold those two codes and then be scanned when the patient needed to provide them in a healthcare facility would ease the user experience and make the whole process much easier.

- **Legislation** - A problem referenced in Section 5.3 is that this prototype is a technical approach to the problem, but has no contact with the legal part of approving an application such as this. Legislation is a gap that can only be filled by approving what can and cannot be done by the healthcare facilities regarding the information that we provide to them using this prototype. Due to this, the prototype currently allows people to carry their own medical files in their personal wallet, but does not prevent healthcare facilities from also keeping the data. The problem of taking power away from these organizations is not solved, but the solution would depend on the legislation around this technology.

- **Stress tests** - As indicated in section 5.2, due to this prototype being a proof of concept, there were actually no stress tests on the network and the prototype application itself. This kind of test is fundamental when developing an application of this sorts and should therefore be done as a next step when continuing the development of this prototype.

- **Encryption optimizations** - AES is one of the most known and reliable methods of encryption, especially considering the nature of the files being encrypted, but the approach to it was simple from a security standpoint. Given this fact, its important that the prototype is futurely updated with more correct, optimized or even newer methods of encryption, in order to maintain safety of the information.

References

[1] Aimedis. https://aimedis.io/about, last accessed 2022-02-28.

[2] Centre of Excellence - BlockChain Technology. https://blockchain.gov.in/bloodbankpage.html, last accessed 2022-02-28.

[3] A Decentralized Gaming Metaverse Made By Players. https://sandbox.game, last accessed 2022-02-28.

[4] What is Ethereum? https://ethereum.org, last accessed 2022-03-01.

[5] What is Fantom? https://admin.fantom.foundation/intro-to-fantom/, last accessed 2022-03-02.

[6] The Difference Between Blockchain and Distributed Ledger Technology, January 2018. https://marcopolonetwork.com/articles/distributed-ledger-technology/, last accessed 2022-02-29.

[7] How Aimedis Wants to Reform the Healthcare System Using Blockchain, July 2021. https://www.coinspeaker.com/aimedis-reform-healthcare-system-using-blockchain/, last accessed 2022-02-28.

[8] Maher Alharby and Aad van Moorsel. Blockchain-based Smart Contracts: A Systematic Mapping Study. *Computer Science & Information Technology (CS & IT)*, pages 125–140, August 2017. arXiv: 1710.06372.

[9] Stefano De Angelis, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, and Vladimiro Sassone. PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain. page 11.

[10] Leemon Baird, Mance Harmon, and Paul Madsen. Hedera: A public hashgraph network & governing council. *White Paper*, 1, 2019.

[11] apostolis banias. What is proof of work?, December 2021. https://banias-apos.medium.com/what-is-proof-of-work-d6f97adecec2, last accessed 2022-02-28.

[12] Federico Matteo Benčić and Ivana Podnar Žarko. Distributed ledger technology: Blockchain compared to directed acyclic graph. In *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, pages 1569–1570, 2018.

[13] JP Buntinx. What is proof of elapsed time. *The Merkle Hash. Available online: https://themerkle. com/what-is-proof-of-elapsed-time/(accessed on 5 December 2019)*, 2017.

[14] Paula Carey. Research: Blockchain and Cryptocurrencies: Coins, tokens, mining and exchanges. `https://library.bu.edu/blockchain_cryptocurrencies/coins`, last accessed 2022-03-01.

[15] Usman W. Chohan. Non-Fungible Tokens: Blockchains, Scarcity, and Value. SSRN Scholarly Paper ID 3822743, Social Science Research Network, Rochester, NY, March 2021.

[16] Claudio Cilli, Giulio Magnanini, Marco Silipigni, and Fabrizio Venettoni. "Safe Prescription": A decentralized blockchain protocol to manage medical prescriptions. March 2021.

[17] Paul Dunphy, Luke Garratt, and Fabien Petitcolas. Decentralizing Digital Identity: Open Challenges for Distributed Ledgers. In *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, pages 75–78, April 2018.

[18] Joshua Ellul, Jonathan Galea, Max Ganado, Stephen Mccarthy, and Gordon J. Pace. Regulating Blockchain, DLT and Smart Contracts: a technology regulator's perspective. *ERA Forum*, 21(2):209–220, October 2020.

[19] Tiago M. Fernández-Caramés and Paula Fraga-Lamas. *Advances in the Convergence of Blockchain and Artificial Intelligence*. BoD – Books on Demand, January 2022. Google-Books-ID: Y7ZaEAAAQBAJ.

[20] Victor Garcia-Font. Conceptual Technological Framework for Smart Cities to Move towards Decentralized and User-Centric Architectures Using DLT. *Smart Cities*, 4(2):728–745, June 2021. Number: 2 Publisher: Multidisciplinary Digital Publishing Institute.

[21] Gerald R. Gray. Immutability and Forks. In Gerald R. Gray, editor, *Blockchain Technology for Managers*, pages 45–52. Springer International Publishing, Cham, 2021.

[22] Houssein Hellani, Layth Sliman, Abed Ellatif Samhat, and Ernesto Exposito. On Blockchain Integration with Supply Chain: Overview on Data Transparency. *Logistics*, 5(3):46, September 2021. Number: 3 Publisher: Multidisciplinary Digital Publishing Institute.

[23] Houssein Hellani, Layth Sliman, Abed Ellatif Samhat, and Ernesto Exposito. Overview on the Blockchain-Based Supply Chain Systematics and Their Scalability Tools. *Emerging Science Journal*, 4(0):45–69, August 2021. Number: 0.

[24] Yarilet Perez Jake Frankenfield, Erika Rasure. What Is Proof of Burn for Cryptocurrency?, September 2021.

[25] Mark Joselli. Blockchain e games. *SBGAMES*, 17:1–11, 2018.

[26] Niclas Kannengießer, Sebastian Lins, Tobias Dehling, and Ali Sunyaev. Trade-offs between Distributed Ledger Technology Characteristics. *ACM Computing Surveys*, 53(2):42:1–42:37, May 2020.

[27] Iuon-Chang Lin and Tzu-Chun Liao. A survey of blockchain security issues and challenges. *Int. J. Netw. Secur.*, 19(5):653–659, 2017.

[28] Alexander Lipton. Blockchains and distributed ledgers in retrospective and perspective. *The Journal of Risk Finance*, 19(1):4–25, January 2018. Publisher: Emerald Publishing Limited.

[29] Debin Liu and L Jean Camp. Proof of work can work. In *WEIS*. Citeseer, 2006.

[30] Duy-Minh Nguyen, Quang-Huan Luu, Nguyen Huynh-Tuong, and Hoang-Anh Pham. Mbpba: Leveraging merkle tree and blockchain to enhance user profile-based authentication in e-learning systems. In *2019 19th International Symposium on Communications and Information Technologies (ISCIT)*, pages 392–397, 2019.

[31] OpenSea. Bored Ape Yacht Club - Collection. `https://opensea.io/collection/boredapeyachtclub`, last accessed 2022-03-01.

[32] Seongjoon Park and Hwangnam Kim. DAG-Based Distributed Ledger for Low-Latency Smart Grid Network. *Energies*, 12(18):3570, January 2019.

[33] Dominic Pirker, Thomas Fischer, Harald Witschnig, and Christian Steger. velink - a blockchain-based shared mobility platform for private and commercial vehicles utilizing erc-721 tokens. In *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*, pages 62–67, 2021.

[34] Witek Radomski. ERC-1155: The Final Token Standard on Ethereum | Enjin Blog, June 2019. `https://enjin.io/blog/erc-1155-token-standard-ethereum`, last accessed 2022-03-01.

[35] Michel Rauchs, Andrew Glidden, Brian Gordon, Gina C. Pieters, Martino Recanatini, François Rostand, Kathryn Vagneur, and Bryan Zheng Zhang. Distributed Ledger Technology Systems: A Conceptual Framework. SSRN Scholarly Paper ID 3230013, Social Science Research Network, Rochester, NY, August 2018.

[36] Sana Sabah Sabry, Nada Mahdi Kaittan, and Israa Majeed. The road to the blockchain technology: Concept and types. *Periodicals of Engineering and Natural Sciences*, 7(4):1821–1832, December 2019. Number: 4.

[37] Fahad Saleh. Blockchain without Waste: Proof-of-Stake. *The Review of Financial Studies*, 34(3):1156–1190, March 2021.

[38] The Sandbox. What is The Sandbox?, October 2021. `https://medium.com/sandbox-game/what-is-the-sandbox-850de68d893e`, last accessed 2022-02-28.

[39] Seq. A Quick Overview of Avalanche (AVAX) and Why You Should Be Paying Attention, October 2021.

[40] A. Shahaab, B. Lidgey, C. Hewage, and I. Khan. Applicability and appropriateness of distributed ledgers consensus protocols in public and private sectors: A systematic review. *IEEE Access*, 7:43622–43636, 2019.

[41] A. Shahaab, B. Lidgey, C. Hewage, and I. Khan. Applicability and Appropriateness of Distributed Ledgers Consensus Protocols in Public and Private Sectors: A Systematic Review. *IEEE Access*, 7:43622–43636, 2019. Conference Name: IEEE Access.

[42] Langston Thomas. CryptoPunks: The Ultimate Guide, September 2021. `https://nftnow.com/guides/cryptopunks-guide/`, last accessed 2022-02-28.

[43] Benjamin D. Trump, Emily Wells, Joshua Trump, and Igor Linkov. Cryptocurrency: governance for what was meant to be ungovernable. *Environment Systems and Decisions*, 38(3):426–430, September 2018.

[44] Qin Wang, Rujia Li, Qi Wang, and Shiping Chen. Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges. *arXiv:2105.07447 [cs]*, October 2021. arXiv: 2105.07447.