STUDIES AND RESEARCH WORKS

A SIMPLE TECHNIQUE TO CREATE NFT

Non fungible token

Author:

ahmed damou mohamed el mostapha
Bendjeddou yasmine
matallah mohamed

supervised by Denis Clos

April 27, 2022

Table of Contents

List of Figures

1 Introduction

Our society has gradually gone digital, allowing a new stage in its history: the digital revolution. The rise of digital technologies, too known as information and communication technologies, is appeared in the 1960s with the Internet and knew how to seduce in a few decades a very large audience. Today we have more than 30 billion devices Internet-connected and estimates tell us an increase of 50 billion by 2025. Every day, more than 2.5 quintillion bytes of data are generated digitally.

The digital world is constantly in motion, sometimes making technologies, that have been part of our daily life for years, obsolete very quickly. In a context where the digital media is constantly evolving and expanding, new issues are constantly appearing and making security a dynamic problem, requiring constant effort. Increasingly present, technologies such as connected objects, make all of our everyday objects potentially vulnerable: our watches, our pens, our refrigerators, our homes, our industries, and even our smarter cities. On the other hand, some technologies promise us a safer future by securing our transactions with technologies such as Blockchain.

Afterward few years the blockchain has been developed and we using it in many things. Here we will be interested to the NFT. We were interested by this topic because it's the evolution and in IT domain, NFTs is being heard. For that we decided to create website which can create NFTs,sell and buy them. So, first we will define what is a blockchain and an NFT, and what is the link between the both, after that we will talk about how we got organized to achieve our objectives, and then we will show the different steps of our work.

2 Blockchain and NFT

2.1 Blockchain

So what is a Blockchain ? A blockchain is a distributed database that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format. They are best known for their crucial role in cryptocurrency systems, such as Bitcoin, for maintaining a secure and decentralized record of transactions.

Blockchain is a type of shared database that differs from a typical database in the way that it stores information, they store data in blocks that are then linked together due to cryptography and blocks have certain storage capacities and, when filled, are closed and linked to the previously filled block, forming a chain of data known as the blockchain.

Different types of information can be stored on a blockchain, but the most common use so far has been as a ledger for transactions.

Figure 1: Blockchain

The announcement of new cryptocurrencies and unique features seems to be growing every day, and it seems every country in the world is showing signs of developing digital versions of their currency, from the digital dollar to the digital yuan.

Blockchain technology started as the underlying technology for cryptocurrency, but it has grown much wider in its applications over the years. It is already shaking up many sectors and revolutionizing the various processes.

There are many platforms of blockchain as we can see on Figure 2.

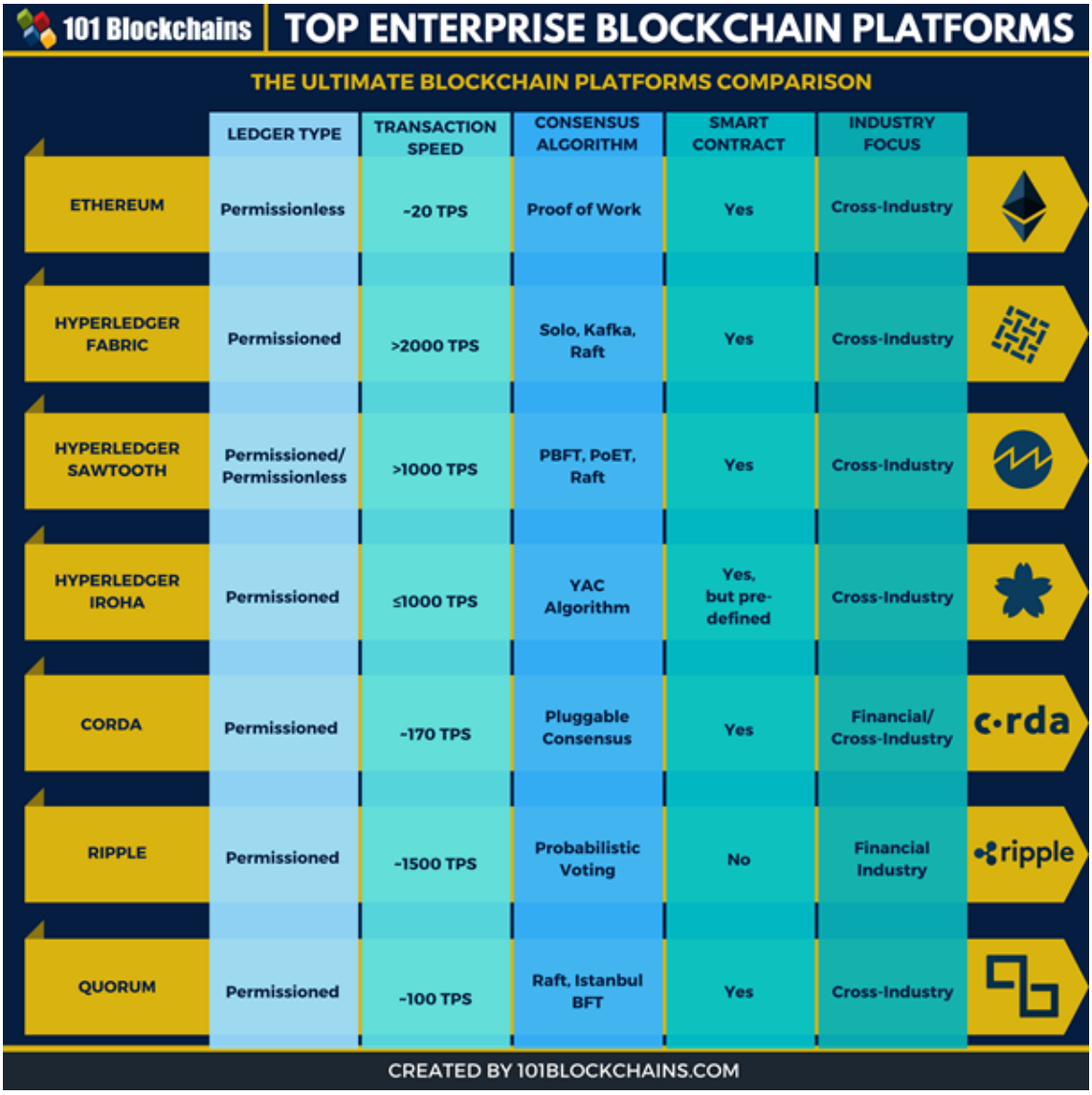


Figure 2: Platforms of Blockchain

Blockchain platforms allow the development of blockchain-based applications. They may or may not be allowed. Ethereum, Hyperledger, Corda, Ripple, and Quorium are a few names that have built blockchain frameworks, allowing people to develop and host applications on the blockchain.

The most widely used blockchain for NFTs today is the Ethereum proto-

col, which requires significant computing power as we can see on Figure 2, less than 20 transactions per second.

2.2 What are blockchains for?

The ability to control and verify the history of an item is a significant feature of blockchains, as it eliminates the need to trust a provider. They enable you to establish ownership or proof of origin in this way.
Blockchain's advantages in the supply chain :
Bitcoin is the most well-known Blockchain implementation. However, Blockchain's distributed ledger properties enable it to help execute and monitor any transaction, not only cryptocurrencies. The deployment of Blockchain in the supply chain is driven by reliability and integrity. The following are some of the highlights:

- Consensus
  All parties must agree for a transaction to be valid. Without this agreement, no new blocks or adjustments are made. This implies that all parties are aware of when a change is being made and have agreed to it. Each transaction is valid if all of the entities in the chain agree. Blockchain technology may be utilized in the supply chain to bring consensus to a wide range of transactions, including payment, warehouse management, transportation, and delivery.

- Provenance
  What is blockchain provenance, and how does it apply to supply chains? In reality, provenance is a key feature in the supply chain. You can know exactly where raw materials or products came from and where they are, professionals can rapidly see who possessed assets and when they did so using provenance. Provenance can be tied to any asset in a supply chain, including iron ore, food, money, machines, and even intellectual property.

- Immutability
  It's nearly impossible to manipulate with a distributed ledger entry. Each entry has many copies, all of which must be updated at the same time. Only a new blockchain transaction can undo the prior one's effect. Implementing blockchain in the supply chain makes falsifying a payment transaction, inventory records, warehousing conditions, deliv-

ery timeframes, and other data extremely difficult.

- Finality: The shared ledger's copies all have the identical version of the truth. Because all parties have a single perspective of the transaction, trust is built. For supply chain management (SCM), blockchain provides a level of certainty that lowers disagreements and allows all stakeholders to build stronger connections.

Key points concerning blockchain applications in a nutshell:

- Blockchains enable connections that are not based on trust.
- They can be used to trace a product's origins.
- They can be used in a variety of ways.
- They are resilient in the face of downtime concerns.

2.3 How do blockchains work ?

A blockchain has a lot of features. To make things easier to understand, we'll start with a very simplistic model and gradually add and explain more aspects as we build up our conceptual model.

At their most basic level, blockchains store data by chunking data into blocks and linking them together. This isn't a brand-new concept in the world of computing. A linked list (fig 3) operates in a similar way at this level, however there are a few key distinctions that we'll go through.

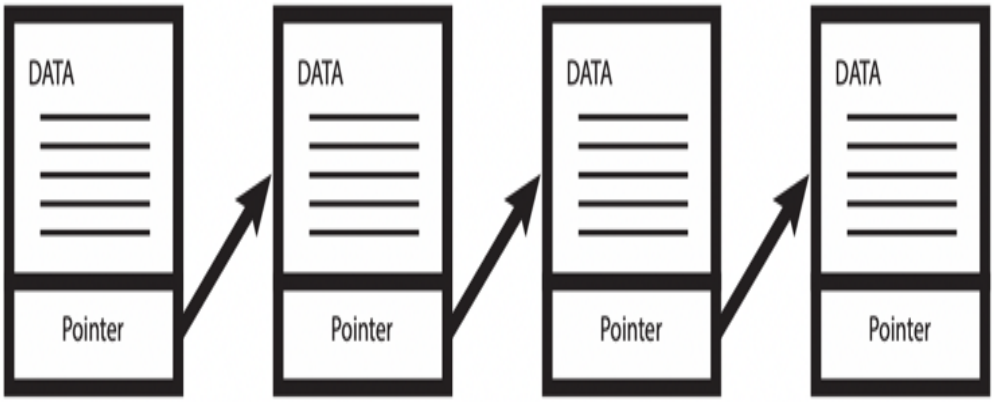


Figure 3: Linked lists

Each node in a linked list contains data as well as a pointer to the next node's location. The way blockchains work is a little different. The contents of a Bitcoin block are depicted in the diagram below (fig 4).

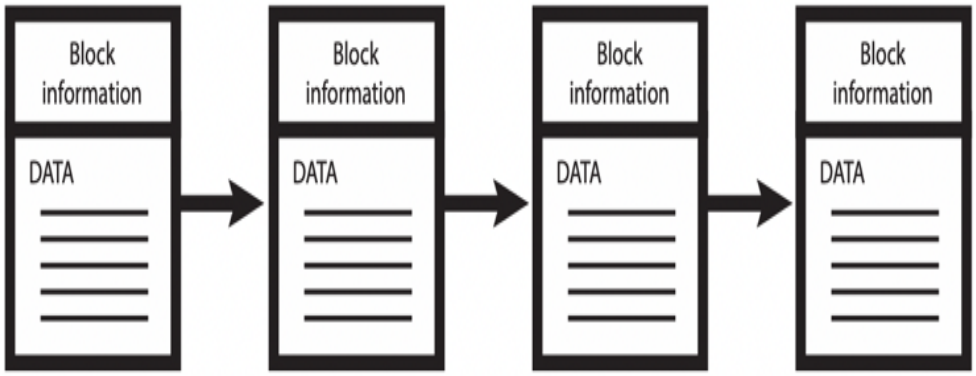


Figure 4: Beginning blockain

Each block in a blockchain has a certain amount of data and is linked to the one before it. Blocks are frequently compared to pages in a book, with

the entire book being the blockchain and the data contained within the page representing the data.

Each block has a header that contains various bits of metadata about the block in addition to the data it contains. As we have a better knowledge of the blocks and the blockchain that they construct, we'll look at the structure of this header.

Files are used to store the blocks. Outside of the chain, they are indexed by a separate index file, which also contains other relevant information for the system. The blkindex.dat file in Bitcoin, for example, comprises an index of the block files. The blk000n.dat file contains block data, where 000n is the block number (fig 5).

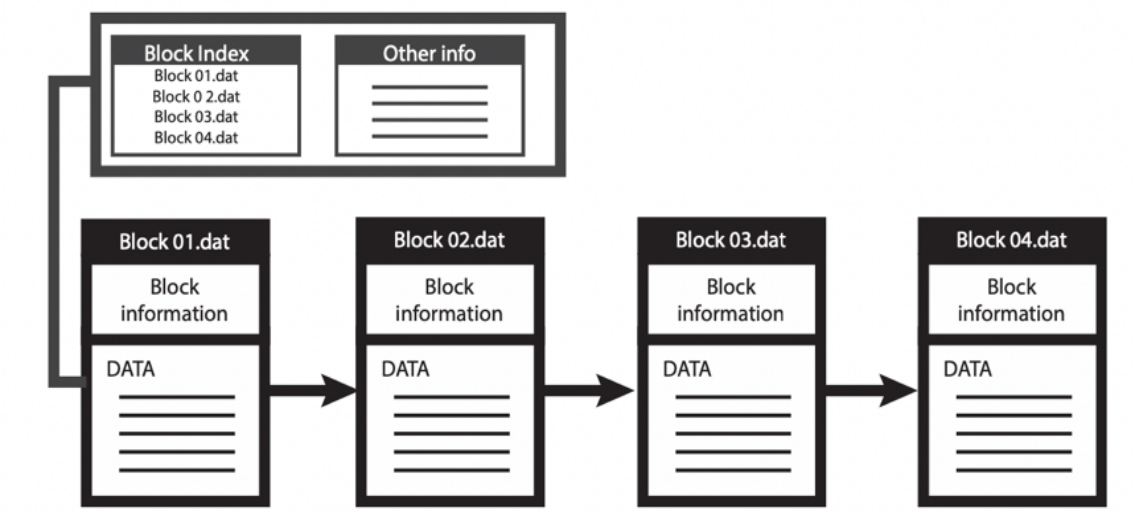


Figure 5: Blockain with index

Let's look at a block in more detail. Each block contains some data, including the block's hash and the preceding block's hash. The data held within a block varies depending on the type of blockchain.
For example, the Bitcoin blockchain contains information about a transaction, such as the sender, receiver, and quantity of bitcoin sent. A hash is a number that can be compared against a fingerprint. It uniquely identifies a block and all of its contents, just like a fingerprint.

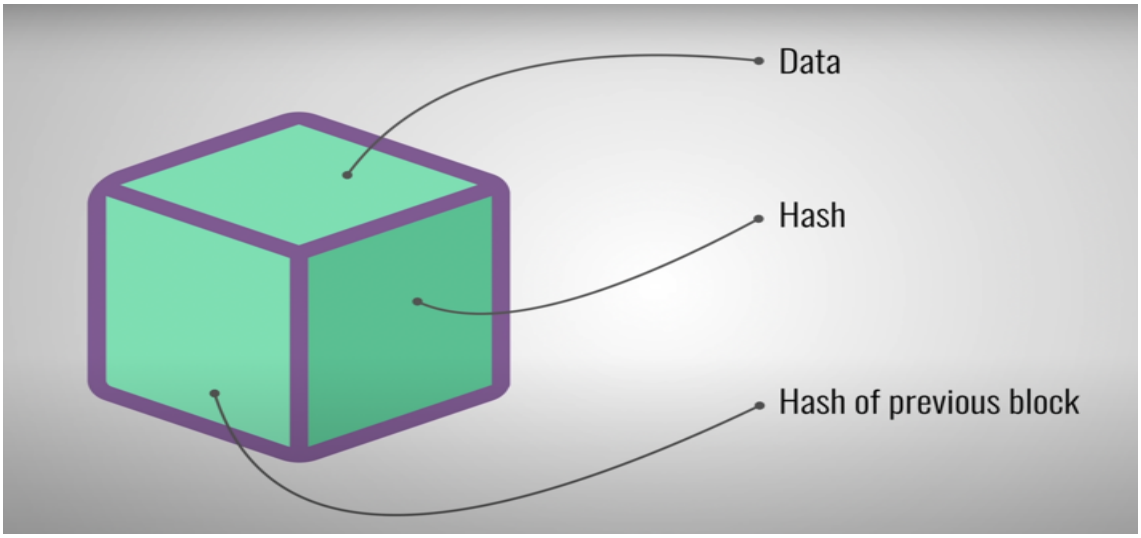


Figure 6: One block of a blockchain

Despite the fact that indexing information is present in blockchains, we will normally leave it out of future diagrams to keep things simple.

Because the link to the next block is separated and the information is indexed in a separate file, the data of the previous block does not need to alter in order to add a point to the next block. A crucial property of blockchains is that they maintain data without changing it.

We know that the data contained in blockchains must be fixed and immutable in order for them to be valuable. Linked lists, on the other hand, do not.

The hash of a block is calculated after it is produced. The hash will change if something inside the block is changed.

In other words, hashes are extremely useful for detecting block changes; if a block's fingerprint changes, it is no longer the same block; the third element inside each block is the hash of the previous block; this effectively creates a chain of blocks; and it is this technique that makes a blockchain so secure. Let's look at an example: we have a chain of three blocks, each of which includes a hash and the previous block's hash, thus block number 3 points to block number 2, and block number 2 points to number 1.

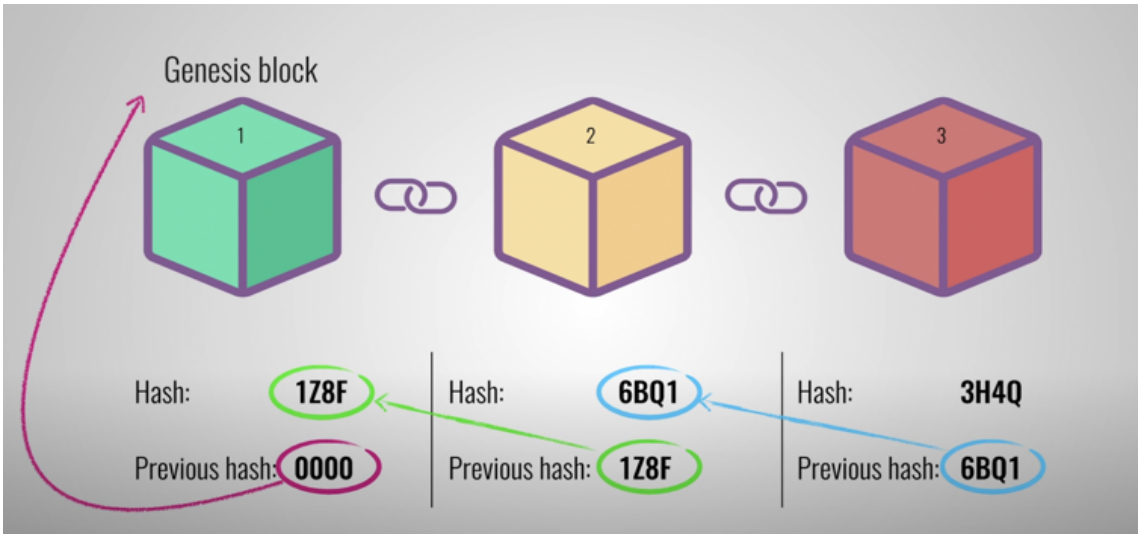


Figure 7: Three blocks of a blockchain

Because it is the first, the first block is unique so it cannot point to prior blocks. Let's imagine you tamper with the second block, which causes the hash of the block to change as well. As a result, block 3 and all subsequent blocks will be invalid since they will no longer store a valid hash of the prior block. As a result, altering a single block invalidates all subsequent blocks.

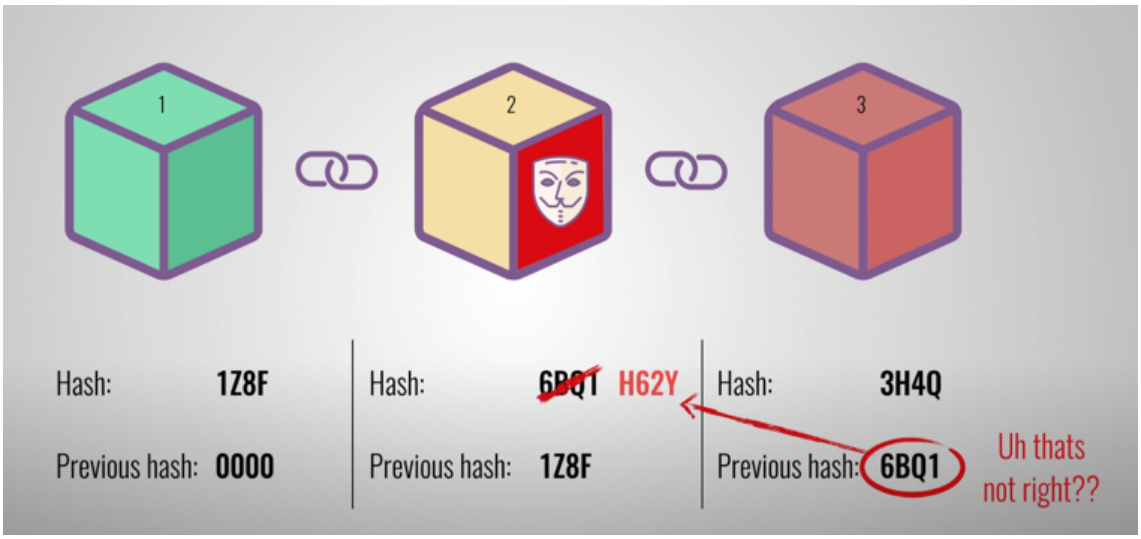


Figure 8: case: integrity of the block 2 is altered.

When someone joins this network, he receives a complete copy of the blockchain,

which the node can use to ensure that everything is still in working order. Let's have a look at what happens when someone makes a new block. Everyone on the network receives the new block. The block is then verified by each node to ensure that it is valid.

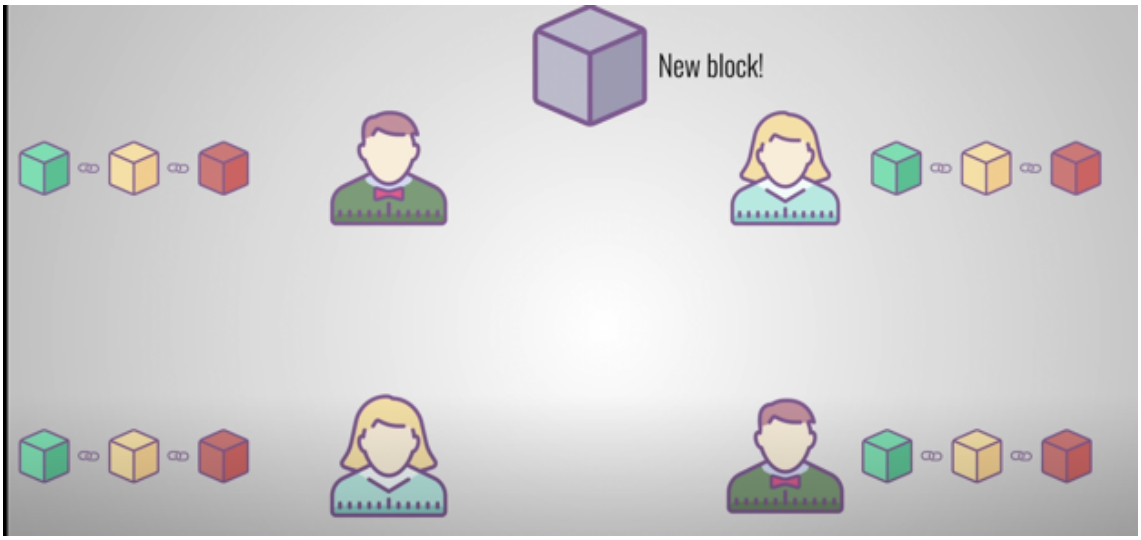


Figure 9: A new block created

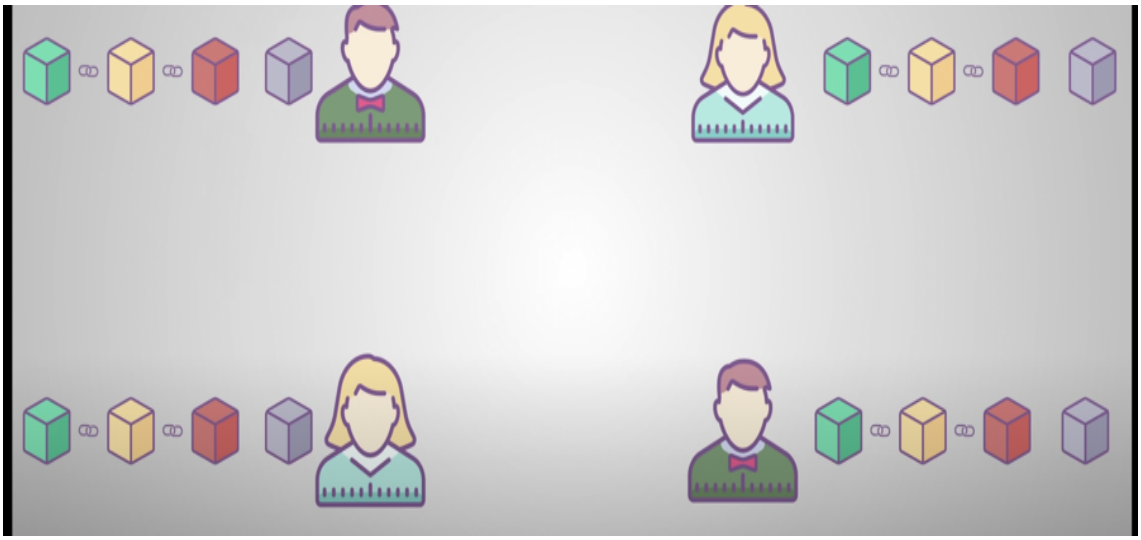


Figure 10: Verification of the new block by nodes

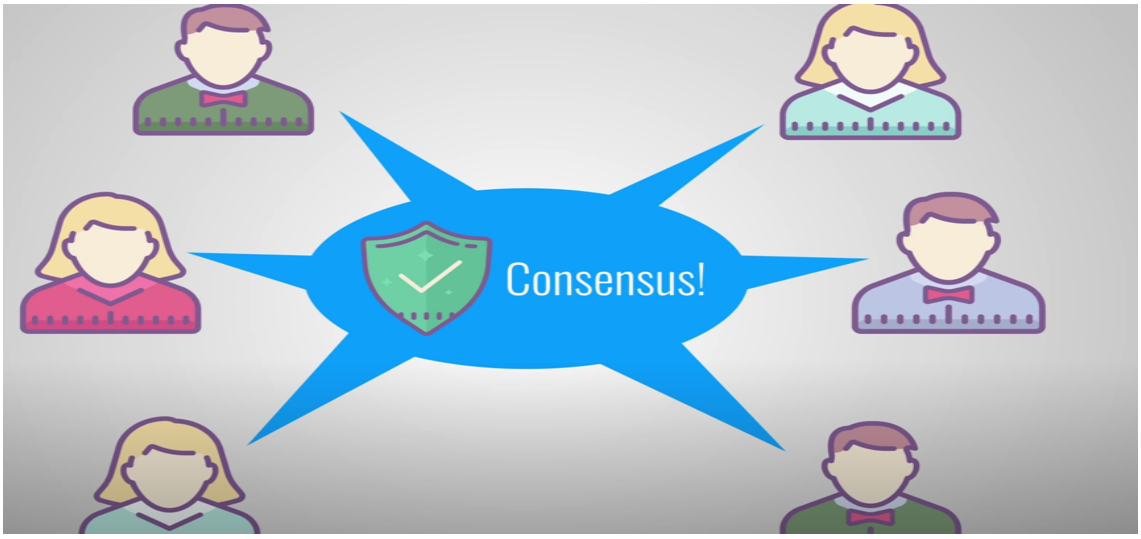


Figure 11: Acceptance of the new block

2.4 Merkle tree

However, hashes alone are insufficient to prevent tampering it's the reason why blockchains use Merkle Trees. Basically a Merkle Tree is a data structure that encodes the blockchain data in an efficient and secure manner. So let's take a closer look at Merkle Trees: A Merkle tree is a hashing algorithm-based structure. It's a tree-like structure in which the leaves are hashes of data, usually depicted upside down from how one may expect a tree to appear. Each of the leaves (at the bottom) is a hash of data, as you can see. Each leaf pair's hash is added together to form the parent node. After that, they're merged to form the next parent node, and so on, until you reach the root. If there isn't a pair to use, the same value is used again, resulting in a different hash. They provide us with a way to check the facts included in the tree. The Merkle root will change if any component of the data is altered. The Merkle root is used in blockchains to allow the system to verify the block's contents. The hashing of the block's contents and links between blocks helps to ensure that if anything changes within any of the blocks, that block becomes invalid and is thus discarded.

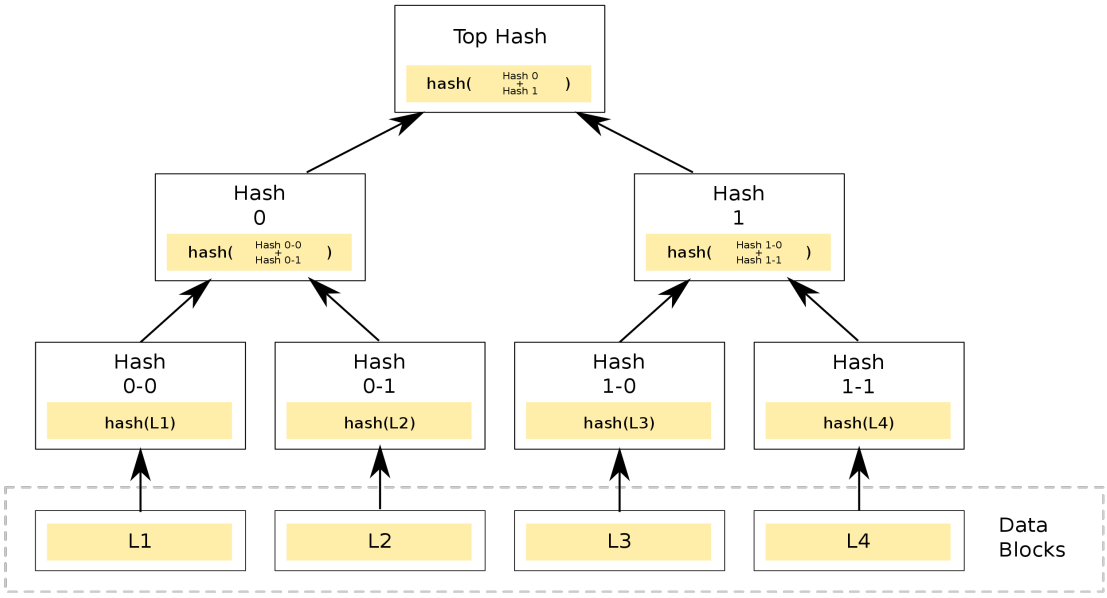


Figure 12: A Merkle Tree

How ever someone could effectively tamper with a block and recalculate all the hashes of other blocks to make the blockchain valid again, thus blockchains feature something called proof-of-work to mitigate this. Basically it's a mechanism that makes the building of new blocks take longer. In the instance of Bitcoin, calculating the requisite proof-of-work and adding a new block to the chain takes roughly 10 minutes. This approach makes tampering with the blocks extremely difficult, because if you tamper with one block, you'll have to recalculate the proof-of-work for all subsequent blocks. A blockchain's security stems from its innovative use of hashing and the proof-of-work method.

This is accomplished by combining two values found within each block: the nonce and the difficulty target.

The nonce :
This is a randomly generated number. The reason it is here is so that one can add different nonce values, and when hashed with the block we will get different hashes as a result. We can generate many different hashes by varying the nonce. As we know, hashes are numbers, even if they don't always appear so when being presented as hexadecimal.

The Difficulty Target :
This is a value that the hash of the block that we want to add, including the nonce, has to be below for the next block to be valid. The Difficulty Target for this block is listed in the previous block. So, say we have a Difficulty Target of 10 and the hash function can produce numbers up to 100. The actual numbers are likely to be a great deal larger than this, but for the sake of simplicity, let's use this as our example.

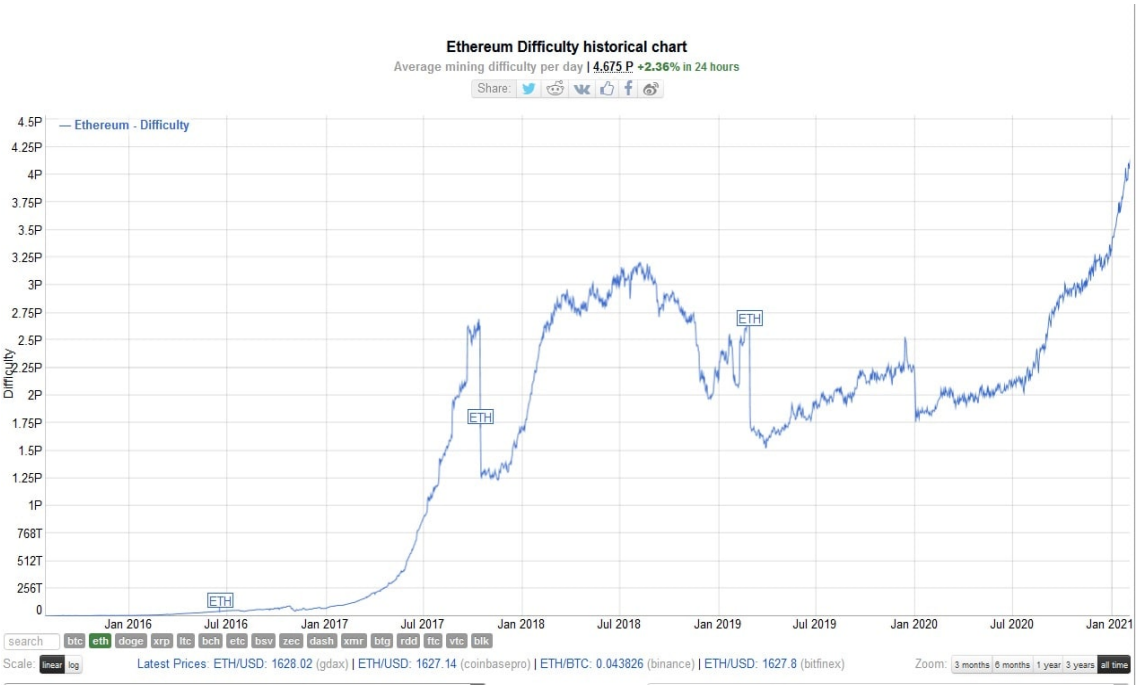


Figure 13: Etherium proof of work performance

But there's another way that blockchains keep themselves safe: they're distributed.

Instead of relying on a central authority to maintain the chain, blockchains rely on a peer-to-peer network that anybody can join.

When someone joins this network, he receives a complete copy of the blockchain, which the node can use to ensure that everything is still in working order.

Blocks that have been tampered with will be rejected by the network's

other nodes. To successfully tamper with a blockchain, you'll need to tamper with all of the chain's blocks, redo each block's proof-of-work, and gain control of more than 50% of the network. Then and only the modified block will be acknowledged by the rest of the world.

This is nearly impossible to accomplish. Blockchains are likewise in a perpetual state of evolution. The establishment of smart contracts is one of the more recent advances. These contracts are basic scripts that may be used to automatically exchange currencies based on certain conditions and are kept on the blockchain. The invention of blockchain technology piqued the interest of many people.

Others soon realized the technology might be used for a variety of purposes, including keeping medical records, creating a digital notary, and even collecting taxes. So now you understand what a blockchain is, how it functions at a fundamental level, and what problems it answers. Let's take a quick look at some hashing methods: Hashing is the term used to describe a procedure in which you enter data and obtain a value in return. Regardless of the quantity of data you input, the output you receive is of a fixed length and always the same length (fig 2.4). A computer algorithm performs the hashing. We can think of them as a black box in general. That is to say, we don't need to be concerned about how this is accomplished on a daily basis; all we need to know is the fundamentals of what is going on. A hash function produces a very large integer, which is commonly represented as an alphanumeric value to make it easier to read, communicate, and deal with.

Figure 14: Determinism of hash function

Key points about hashes:

- They are easy to produce.
- They are effectively one-way.
- They are the same every time for the same data.
- Matching hashes mean we can assume the data is the same.

2.5 Blockchains and hashing

Hashing is used in a variety of ways in blockchains,they also utilize hashing to ensure that data on the blockchain is not altered after it is written.
Let's start with the most basic implementation, except for the first block, which has no prior block, each block includes a hash of the contents in the previous block, instead of a string of zeros, this is known as the genesis block When a new block is added, the preceding block's hash is taken and written into the new block.This means that if the information in block two, for example, was changed the hash of that block would change as well.This implies that the information listed for that block would now be erroneous, invalidating the subsequent block..
If we go back even farther and change something in block one, it will change

its hash, invalidating the following block since its hash will now be changed, invalidating the next block to the present block. It is no longer possible to update the content of any block without invalidating all subsequent blocks. This does not prevent tampering or produce the immutable data storage that blockchain provides, but it is a critical first step. It would be conceivable to change the hashes in the entire chain at this point in our blockchain adventure.
In most cases, blockchains contain far too much data to function in the same way as linked lists. In a short period of time, if each block included only one piece of information, the blockchain would become cumbersome. Instead, each block's information is a chunk of data. Each item in this chunk is hashed as well, to prevent a single value from being changed. This is saved in the block as the Merkle root of the items Merkle tree. Let's take a closer look at what that entails Points to remember:
• Blockchains are chains of chunked data that use hashing.

• The hash of the block is stored in the next block to help prevent later changes.

• Hashing is a one-way process that provides a digital fingerprint of the data.

• It is almost impossible to work out the original data from its hash.

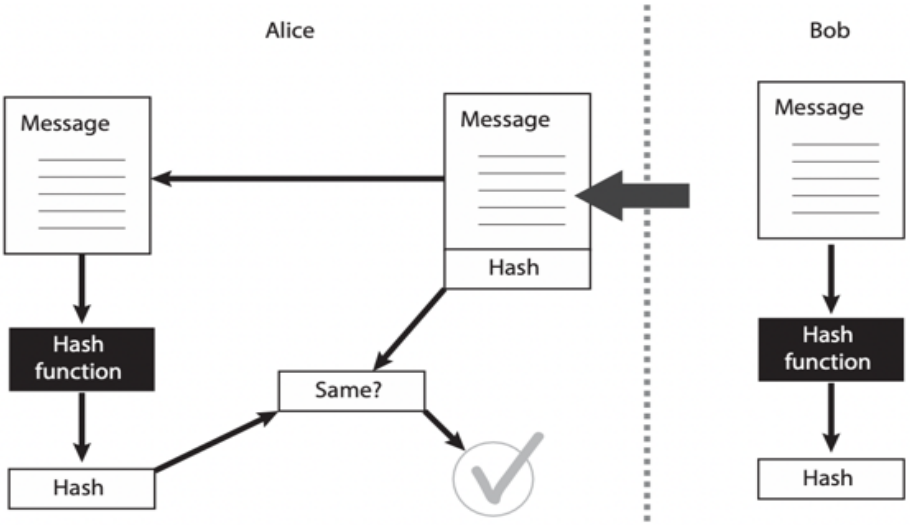
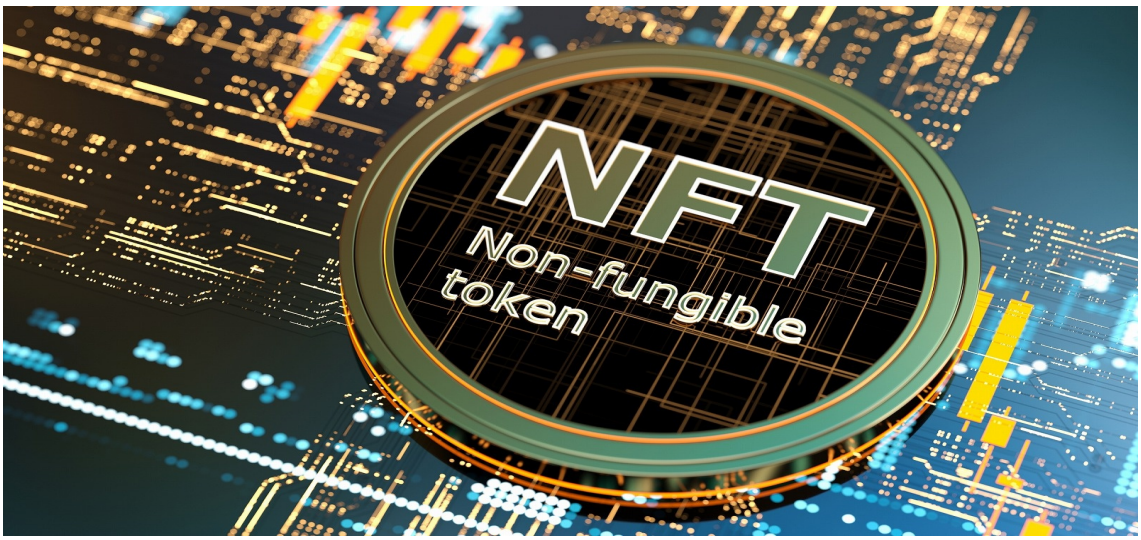


Figure 15: Hash function

2.6 NFT: Non Fungible Token



NFTs are tokens that we can use to represent possession of unique items. They let us symbolize things like art, music, in-game items and videos. They can only have one official owner at a time and they are secured by the Ethereum blockchain: no one can modify the record of ownership or copy/paste a new NFT into existence. So NFTs are unique cryptographic tokens that exist on a blockchain and cannot be replicated. NFTs use blockchain technology to provide verifiable proof of ownership of the item the NFT is associated with. Essentially, is a digital certificate of authenticity.

"Tokenizing" these real-world tangible assets makes buying, selling, and trading them more efficient while reducing the probability of fraud. They are bought and sold online, frequently with cryptocurrency, and they are generally encoded with the same underlying software as many cryptos. NFTs can also function to represent individuals identities, property rights, and more.

Although they have been around since 2014, NFTs are gaining notoriety, because they are becoming an increasingly popular way to buy and sell digital artwork. A staggering price of 174 million dollars has been spent on NFTs since November 2017.

Anyone, from artists to entrepreneurs, authors, or social media personalities, can create an NFT. No experience is necessary, and as long as someone can prove they created or legally own the content, they can create an NFT.

But what is the goal of owning an NFT ? The goal of creating NFTs was to add an element of rarity to what is effectively a limitless resource.

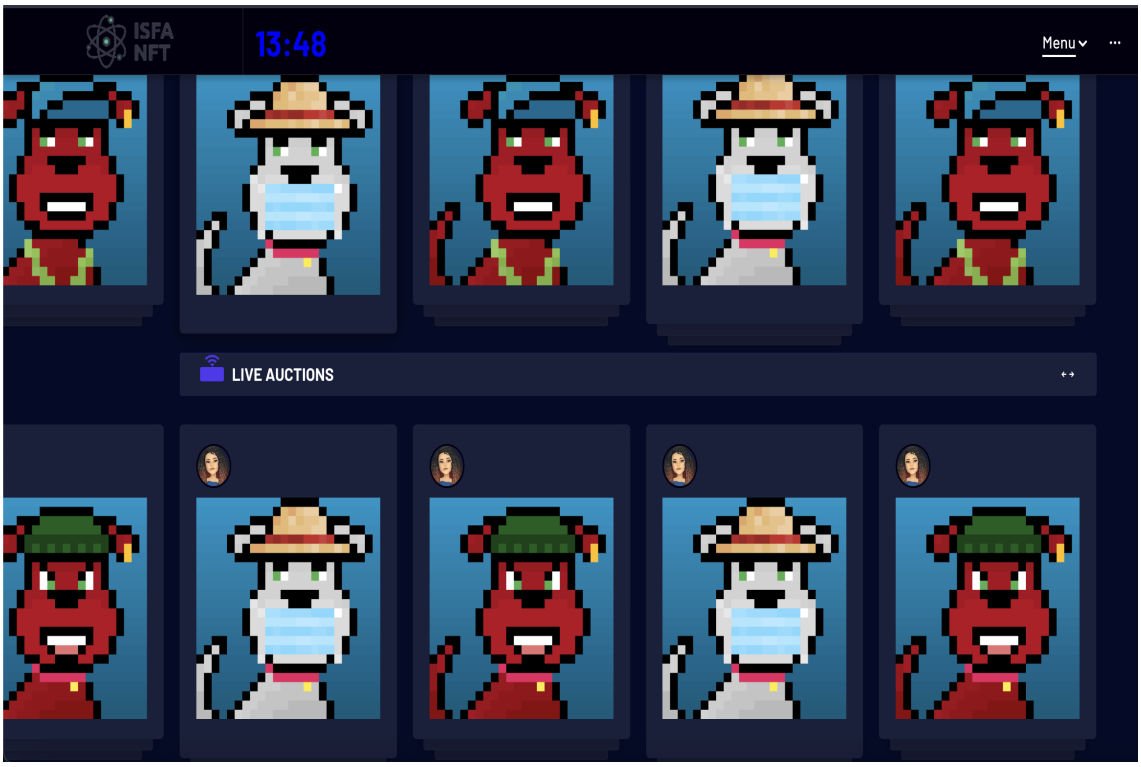


Figure 16: NFT sale example

2.7 How do NFTs work?

NFTs differ from ERC-20 tokens such as DAI and LINK in that each token is totally unique and cannot be divided. NFTs allow for the assignment or claim of ownership of any unique piece of digital data, which can be tracked using Ethereum's blockchain as a public ledger. As a representation of digital or non-digital assets, an NFT is created from digital items. An NFT could, for example, represent:

GIFs are collectibles in the world of digital art. Music Tickets to a live event in the real world Invoices that have been tokenized Documents of legal significance Signatures Videos There are a plethora of new possibilities to explore! At any given time, an NFT can only have one owner. The uniqueID and metadata that no other token can replicate are used to manage ownership. Smart contracts that assign ownership and govern the transferability of NFTs are used to create them. When someone generates or mints an NFT,

they are executing code from smart contracts that follow various standards, such as ERC-721. This data is stored on the blockchain, which is where the NFT is handled. From a high level, the minting process includes the following steps:

Adding a new block to the game Information verification NFTs have certain unique qualities when it comes to storing data on the blockchain:

Each token has a distinct identification that is tied to a single Ethereum address. They are not replaceable 1:1 with other tokens. One ETH, for example, is identical to another ETH. With NFTs, this isn't the case. Each token has a unique owner, whose identity can be easily verified. They are based on Ethereum and may be purchased and traded on any Ethereum-based NFT exchange. To put it another way, if you own an NFT, you can simply verify it. Demonstrating that you hold an NFT is equivalent to demonstrating that you have ETH in your account. Let's imagine you buy an NFT and have the ownership of the one-of-a-kind token transferred to your wallet via your public address. The token verifies that your digital file copy is the original. Your private key serves as verification that you hold the original. The public key of the content author serves as a certificate of authenticity for that specific digital object. The public key of the originator is inextricably linked to the token's history. The creator's public key can be used to prove that the token you own was generated by a certain person, increasing its market worth (vs a counterfeit). Signing messages to confirm you possess the private key behind the address is another technique to prove you own the NFT. Your private key serves as proof of ownership of the original, as previously stated. This indicates that the NFT is controlled by the private keys behind that address. A signed message can be used to prove that you own your private keys without disclosing them to others, as well as proving that you own the NFT! It cannot be manipulated in any way. You can sell it, and in some situations, resale royalties will be paid to the original inventor. Alternatively, you can keep it indefinitely, safe in the knowledge that your Ethereum wallet will protect your investment. Also, if you make an NFT:

You may easily establish that you are the creator. The scarcity is determined by you. Every time it is sold, you can receive royalties. You can sell it on any NFT or peer-to-peer exchange. You're not tied to any particular platform, and you don't require anyone to act as an intermediary. The primary distinction between NFTs and Smart Contracts is that NFTs are enabled by smart contracts that deal with transferability and ownership confirmation. A smart contract, on the other hand, is an application that runs on the Ethereum blockchain.

Definition of a Smart Contract One of the most powerful aspects of blockchain technology is smart contracts. A smart contract is a type of

digital contract in which the details of the agreement between the parties are written in code. When a set of predetermined circumstances are met, a smart contract can also be configured to execute itself. On decentralized and distributed blockchain networks, smart contracts exist. Several organizations are working to develop smart contracts that will stand up in a court of law. The solutions will most likely take the form of smart contract interfaces, in which the code in a smart contract generates a plain-English text outlining the contract's terms. When smart contracts are executed, they can be programmed to activate other smart contracts or create new events. Assets, NFTs, and cryptocurrencies can all be held in smart contracts. When a set of conditions are met based on the code defined in the contract, these assets can be dispersed upon execution.

3 Objectives and organization

3.1 Objectives

In the beginning, to make our NFT project, we decided to create an NFT website named **ISFA NFT** in which, we can register, create NFTs and sell them. At the opening of an account, a certain sum of money is offered to the subscriber. With this money the person can buy NFTs released, by other subscribers, on the sales page of our website.
We wanted to put a condition to buy an NFT, which is that people can't sell their NFTs if they were not created on our site. For the creation of the NFT, we wanted to use a blockchain with limited backup capacity, which means that people can create NFTs as long as the blockchain isn't full. Otherwise, we get into a stock market spirit where NFTs will see their price increase or decrease over time. We found interesting to add a graphic which represent the stock price of the market.

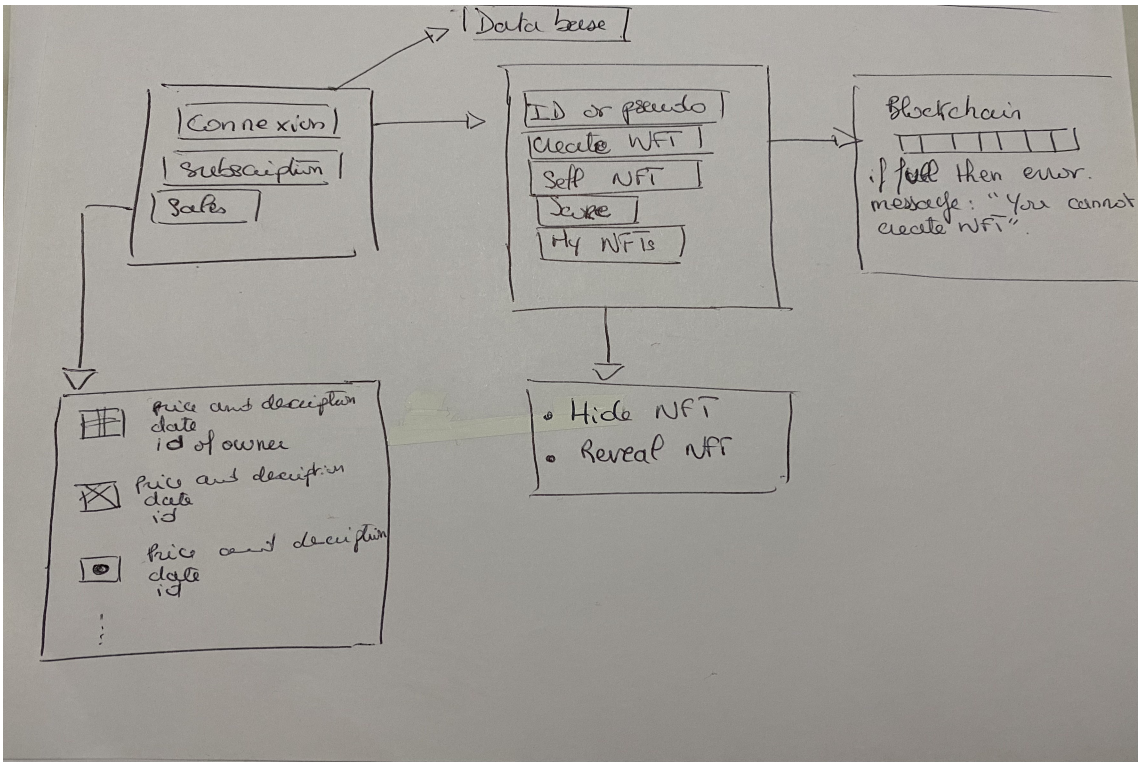


Figure 17: Our Objectives

All information entered are saved in a database which is connected with the

site. To make all this, we decided to use as programming languages: HTML and CSS for the **front-end**, **PHP** and **SQL** for the **back-end**, **JavaScript** for creating NFTs, using case APIs. We also wanted to host our site on the server of the university, and use **React**, which is a JavaScript library which simplifies the creation of interactive user interfaces, and when our data (prices of NFTs over time) changes, React will optimally update the components that need it.

3.2 Organization

For the organization of group work, we created a discord and WhatsApp group to discuss the distribution of tasks, but also to discuss the difficulties that we could encounter, in particular to send us links that we thought were interesting for the work on the project. So to make the NFT site, we had to divide the tasks into three parts: NFT, Back-end and Front-end.

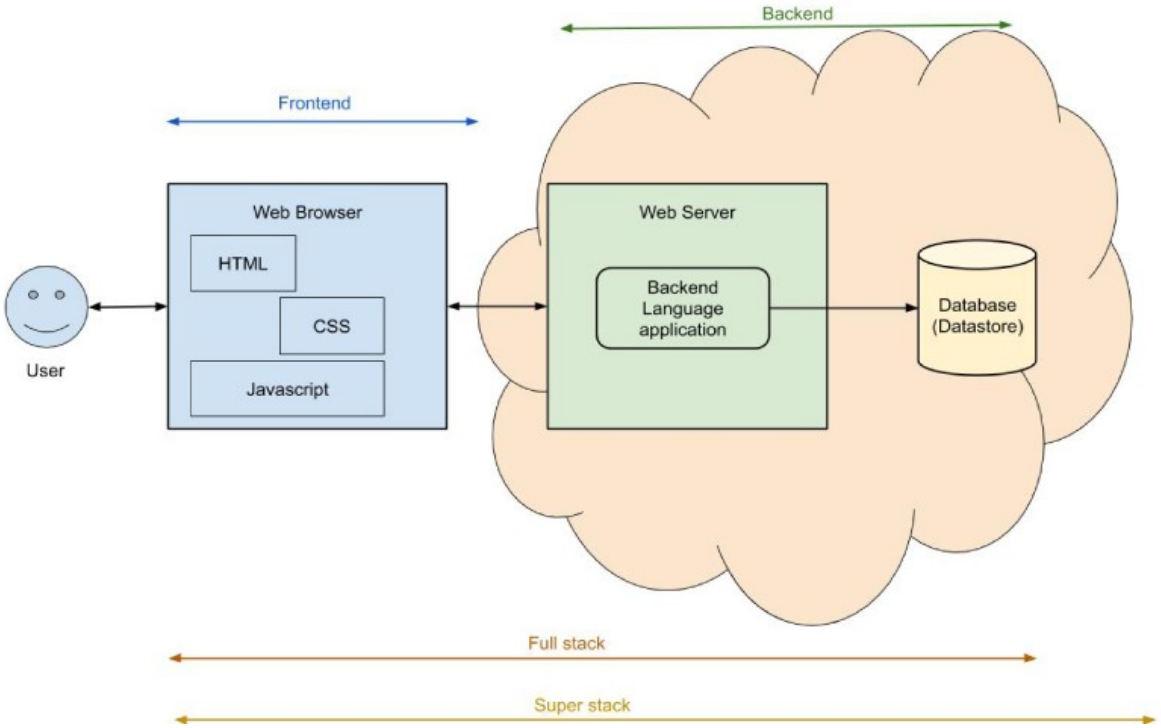


Figure 18: back and front-end notion

First, we decided to use **Django**, an open source python web development framework, for its graphical level performance. Django aims to make web development simple and fast. We tried to learn how to use it but we found that it taking a long time to assimilate everything we needed to put it into practice. Therefore, we tried to use**Brython**, designed to replace JavaScript as the scripting language for the Web. It is a **Python 3** implementation adapted to the **HTML5** environment. In fact, it was easier than Django but we thought it was better using directly **PHP** and JavaScript, so that's what we did.
Later, we had to make changes on our core ideas, instead of using case APIs, we tried to develop the NFT on Python, but we keep using JavaScript for the back-end. In summary, we used SQL for the database using MySQL, Python for the NFTs and JavaScript, HTML, PHP and CSS for front-end and back-end. We add a logo in matrix format. Now, let's show you how we put all this together.

4 ISFA NFT

To make ISFA NFT, each of us worked on a specific part, as I said before. Let's start with the back-end and NFTs part.

4.1 Back-end and NFTs

To make the website, we had to download MAMP, which is a local server environment, there are MySQL and Apache servers we needed. So, we started by creating a database on phpMyAdmin where we put tables:

- Photo that corresponds to the NFTs, it takes as attributes:
  - NFT ID and name.
  - Description.
  - An image ie the NFT.
  - A category that corresponds to the price category(optional because we didn't used it in the end).
  - The owner's id.
  - Visible attribute to say if we want or not make the NFT visible on the market(sale page),

◊ Price of NFT.

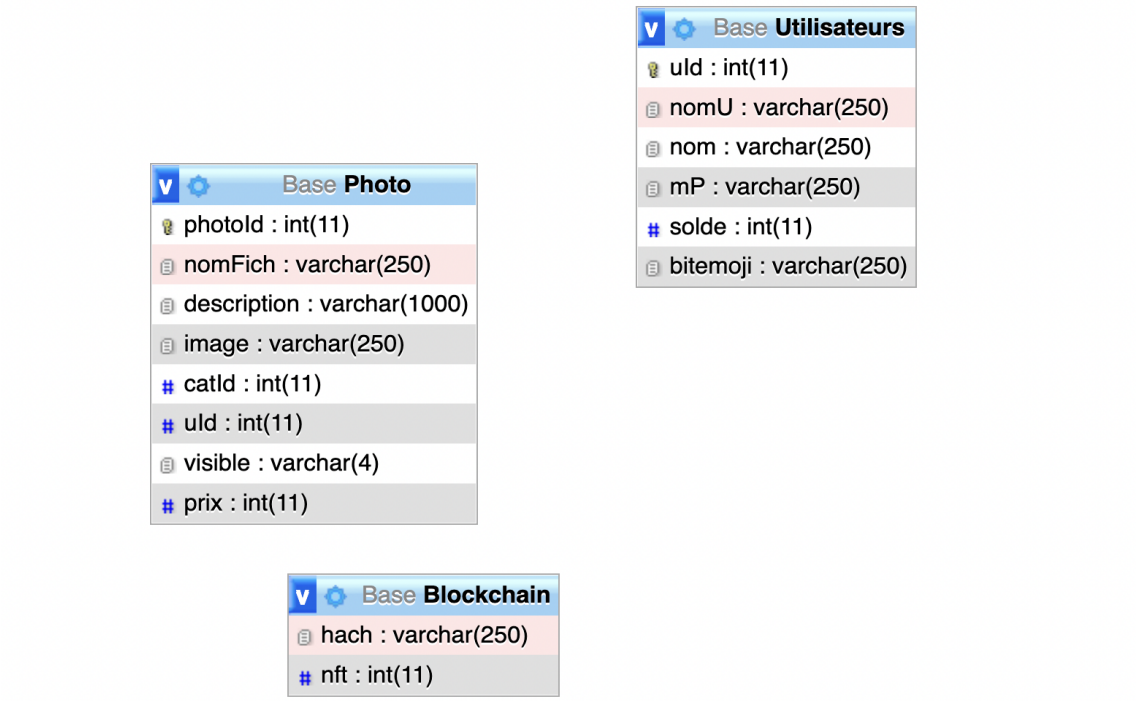


Figure 19: Database

■ Users:

◊ User ID and name.

◊ Password that correspond to the hash of the user's password.

◊ Solde ie the total of the money the user have in the account and bitmoji.

■ Blockchain

◊ NFT ID.

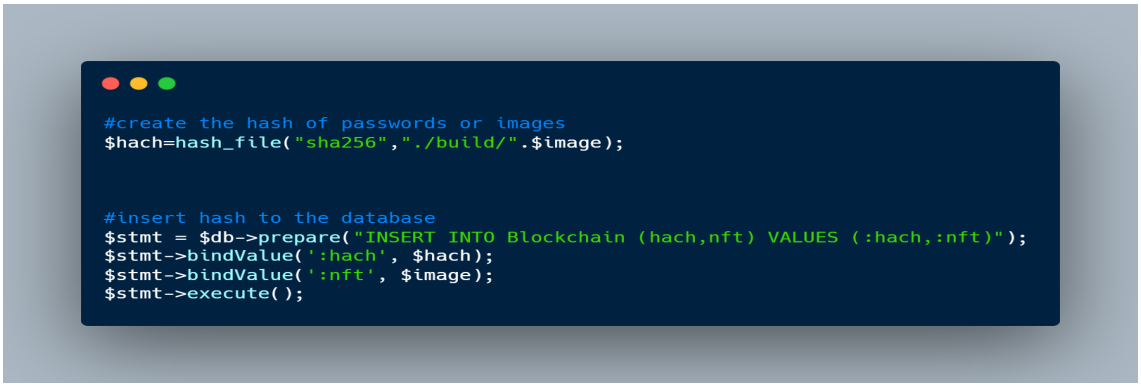
◊ the hash of the image of NFT.

Once the database was created, a script has been made to connect to the database directly, so all the data the user enters on the site will be automatically stored in the database. There is few lines of the script concerning the connection to the database.

```php
public static function beginTransation(){
        self::$connection->beginTransaction();
    }

    public static function commit(){
        self::$connection->commit();
    }

    public static function connect()
    {
        if(self::$connection == null)
        {
            try
            {
                self::$connection = new PDO("mysql:host=" . self::$dbHost . ";dbname=" . self::$dbName ,
self::$dbUsername, self::$dbUserpassword);
            }
            catch(PDOException $e)
            {
                die($e->getMessage());
            }
        }
        return self::$connection;
    }

    public static function disconnect()
    {
        self::$connection = null;
    }
class Database
{
    private static $dbHost = "localhost";
    private static $dbName = "Base";
    private static $dbUsername = "root";
    private static $dbUserpassword = "root";
```

Figure 20: Connection to the database

As I mention it before, we had hashed passwords of users and images of NFTs and we stocked them on the database. Password hashing is used to verify the integrity of your password, sent during login, against the stored hash so that your actual password never has to be stored.



```php
#create the hash of passwords or images
$hach=hash_file("sha256","./build/".$image);


#insert hash to the database
$stmt = $db->prepare("INSERT INTO Blockchain (hach,nft) VALUES (:hach,:nft)");
$stmt->bindValue(':hach', $hach);
$stmt->bindValue(':nft', $image);
$stmt->execute();
```

Figure 21: Hashing passwords and messages

hach	nft
9708890a13372e8d307d6181b8b9cf37ce0141841f61c62b49...	1
9708890a13372e8d307d6181b8b9cf37ce0141841f61c62b49...	2
8d961c961c9b960fc37319affd894e311b160551f303b00976...	3
56995a85d686e112bccacc19adde504317d3129e9fa4fe5264...	4

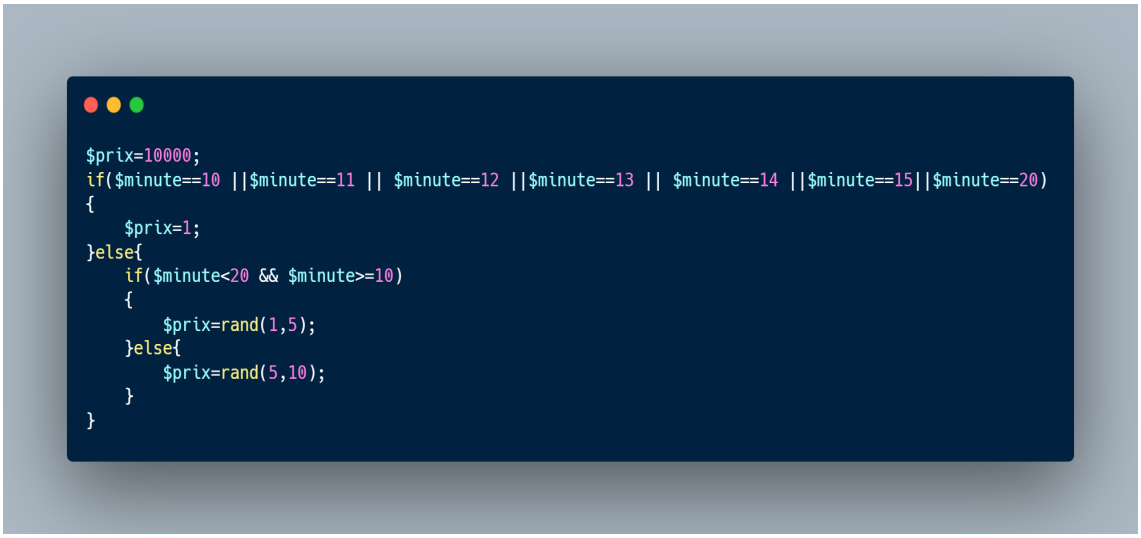
Figure 22: Database: hash of images

After the database we implemented the NFT in python, in our case the NFT are images that are put in a folder and that are drawn randomly and in a unique way, when the user requests the creation of NFT.
We have added an option on the site that gives the user the possibility to check the authenticity of an NFT that they deem false or not authentic. So they can save it and test it on the site. And it's here that the hash of the image will intervene, this means that if the image corresponds to a hash already present in the database then this Nft is authentic and we will display who it belongs to, otherwise if it is not authentic that would mean that the NFT is not registered on the blockchain.

```
$stmt=$db->prepare("SELECT * FROM Blockchain  WHERE hach = :hach");
            $stmt->bindValue(':hach', $hach);
            $stmt->execute();

            $i=0;
            while($res=$stmt->fetch())
            {
                $i++;
            }

            if($i>0){

                $stmt=$db->prepare("SELECT U.* FROM Blockchain B JOIN Photo P ON B.nft=P.photoId JOIN
Utilisateurs U ON P.uId=U.uId WHERE hach=:hach");

                $stmt->bindValue(':hach', $hach);
                $stmt->execute();
                echo '</br>';

                $result=$stmt->fetch();
                $uid=$result['uId'];
                $message="The ID of the owner of this NFT IS ".$uid;

           ;

            }else{

                $message="This NFT is not registred  ";

            }
```

Figure 23: Code that manages authenticity

Until now we have only talked about the security of the NFT site. Now let's move on to how the site works. At the creation of an account, a sum of 10 Ter is offered (Ter is a currency here), with this sum the user can buy or create NFT which are paying in both cases. More explicitly, the creation of an NFT by a user means that he buys an NFT from the system. The system sets prices randomly based on time. For this, a countdown has been set. The price of the NFT varies according to the countdown.



```
$prix=10000;
if($minute==10 ||$minute==11 || $minute==12 ||$minute==13 || $minute==14 ||$minute==15||$minute==20)
{
    $prix=1;
}else{
    if($minute<20 && $minute>=10)
    {
        $prix=rand(1,5);
    }else{
        $prix=rand(5,10);
    }
}
```

Figure 24: code of variation of price

When the countdown is at 10 or 11 or 12 or 13 or 14 or 15 or 20 minutes then the price of the NFT is 1 Ter, if the number of minutes is between 10 and 20 then the price varies from 1 to 5 Ter, otherwise it varies between 5 and 10 Ter. For every creation of NFT, the system stock the selling price in a price.txt file.
Once the NFT is created, the owner who is now registered on the blockchain, can either sell his NFT, at the price he wants, by putting it on the Market page or hidden it from the page if he doesn't want to sell it. He can also donate it to a person on condition that he knows his ID, he can even make money transfers to another user. Now, let's see what this all looks like.

4.2 Visual of the site

The site has a homepage where we find a graph describing the evolution of the price of NFTs, a countdown, an NFT showcase, to see the NFT put on the market, there is also a menu.

Figure 25: Nft shawcase

In the menu we have several options:

◊ Connection.

◊ Registration: as we have already said all the data are recorded in the database.

◊ Market or sales page: we find the details of NFTs that are for sale but we cannot buy if we are not connected.

◊ Information about us

◊ Verification of the authenticity: if someone have a doubt about an NFT he can check it.

After logging in, we have access to all our NFT, and being owner, we can change the sale price, we can give an NFT to someone who will become the new owner of this NFT, and we can decide if we want to hide it or make it visible on the market.

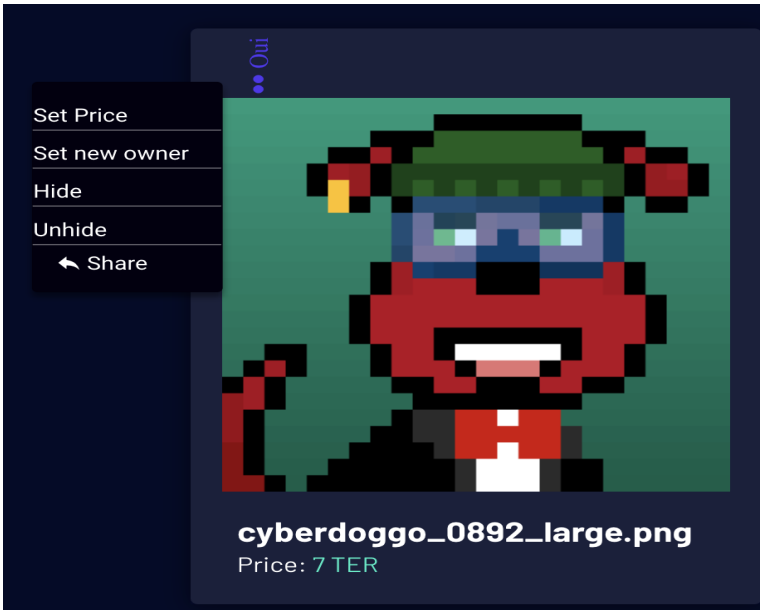


Figure 26: Options of the owner of an NFT

Obviously for the purchase of an NFT or a money transfer, the user must have a sufficient balance otherwise an error message is displayed.

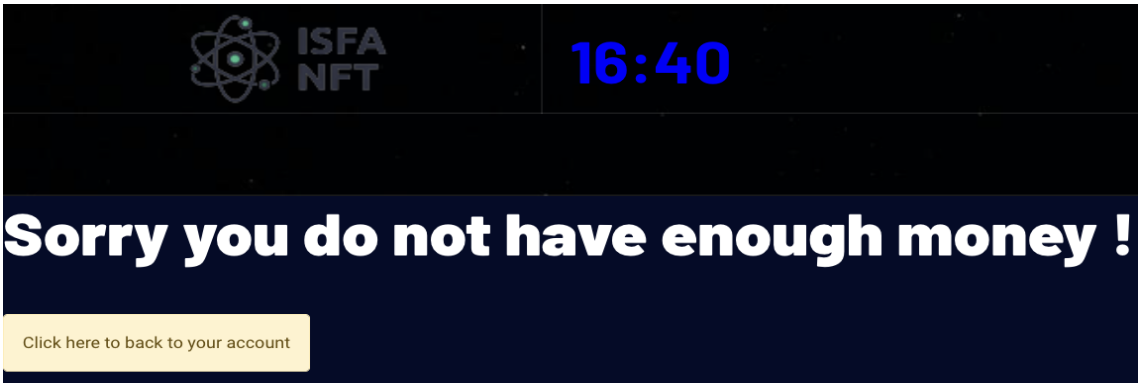


Figure 27: Error message for insufficient balance

You now have all the information about our site, so come create your NFT and become rich!!

5 Conclusion

To conclude, this studies and research have allowed us to learn a lot of things, both in the field of NFTs and the Blockchain but also in the field of development. We were able to deepen our knowledge of blockchain because, even if it was being heard a lot, we knew very little about it.
The NFTs have become important in today's life, everyone wants to own an NFT and for that people are ready to pay exorbitant amounts.
Just like cryptocurrency, money is the primary reason for purchasing NFTs. Buyers of digital art favor speculation over the artistic interest of the work. A study show that, for buyers who spent at least $25,000 on NFT, 95% said that "return on investment was their main motivation". It's certainly tempting but we have to keep in mind that it's a double-edged sword, either it enriches or it ruins us.

6 ANNEX

Links:

https://www.youtube.com/watch?v=2VtH-XAOjXw

https://www.youtube.com/watch?v=0uYJQpuNxDs

https://www.investopedia.com/terms/n/nonce.asp#:~:text=Nonce%20in%20Cryptocurrency%3F-,A%20nonce%20is%20an%20abbreviation%20for%20%22number%20only%20used%20once,in%20order%20to%20receive%20cryptocurrency

https://www.youtube.com/watch?v=YIc6MNfv5iQ

https://www.youtube.com/watch?v=ZE2HxTmxfrI

https://www.youtube.com/watch?v=SSo_EIwHSd4

https://www.lefigaro.fr/secteur/high-tech/l-argent-premiere-motivation-d-achat-d

https://smallbiztrends.com/2022/01/how-to-make-an-nft.html

https://www.theverge.com/22310188/nft-explainer-what-is-blockchain-crypto-art-fa

https://ethereum.org/en/nft/

https://beaubourg-avocats.fr/nft/

https://www.sciencealert.com/what-are-non-fungible-tokens

https://we.tl/t-IaWl3cO48m

Books:

-A. Summers - Understanding Blockchain and Cryptocurrencies_ A Primer for Implementing and Developing Blockchain Projects (2022)
-Juan Jiménez - A Guide to Crypto Collectibles and Non-fungible Tokens NFTS (crypto, cryptocurrency, polkadot, trading, bitcoin, staking, earn
-Andreas M. Antonopoulos - Mastering Bitcoin: Programming the Open Blockchain Broché – 16 juin 2017

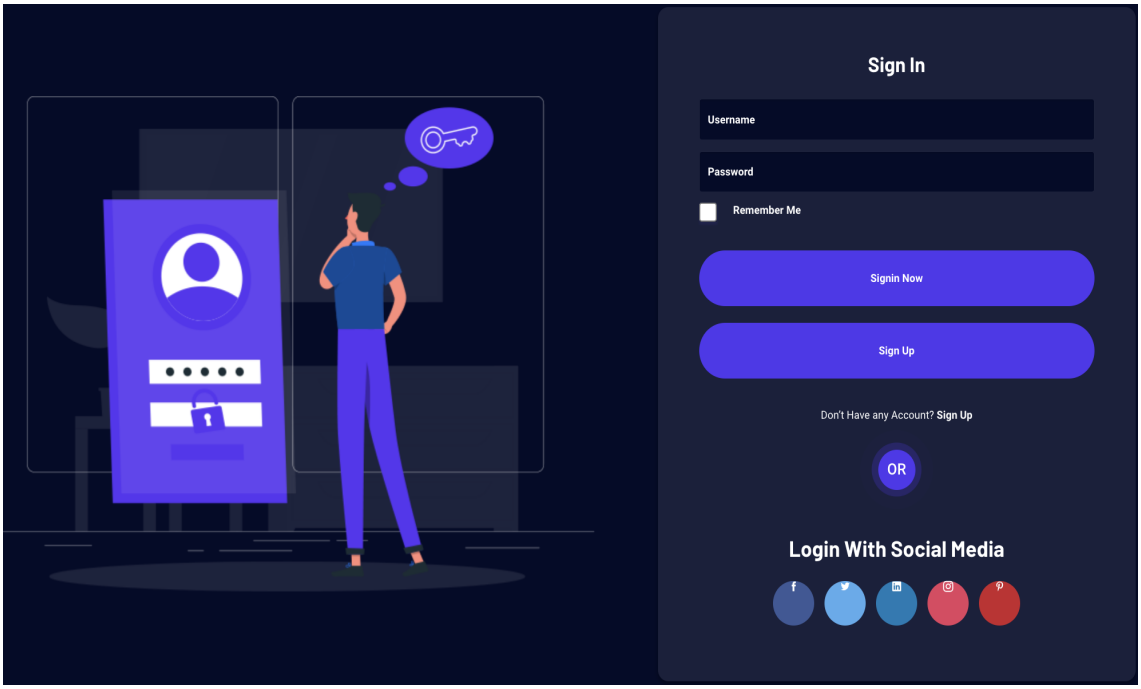
Website:

Logo of our site:

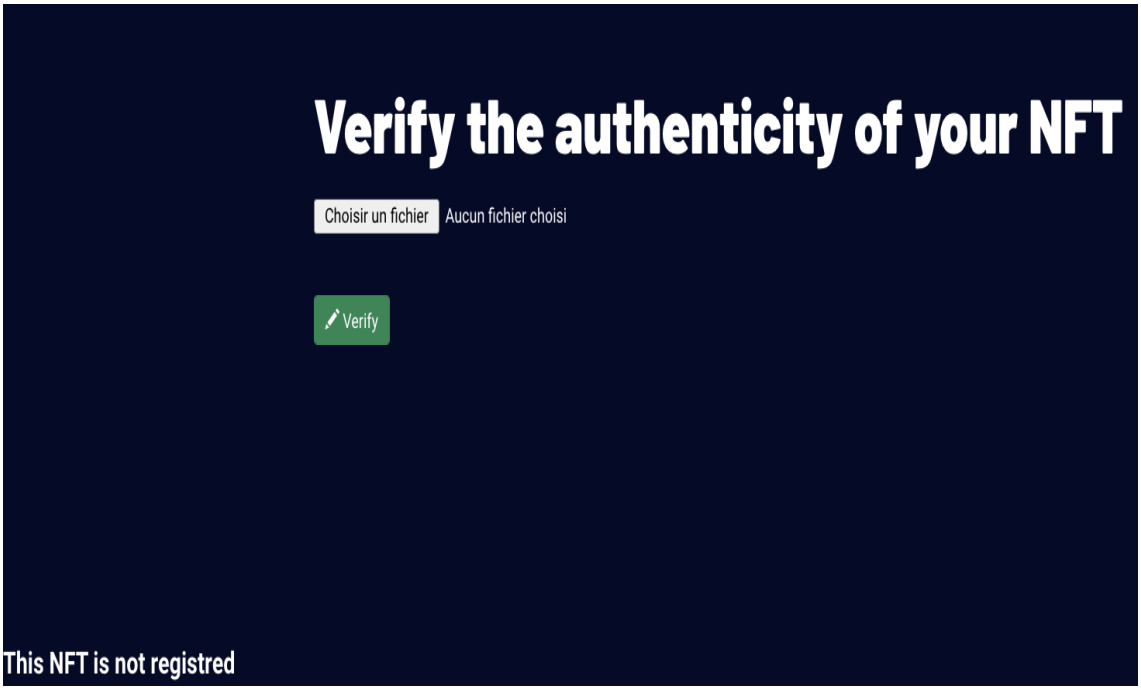
ISFA
NFT

Homepage of the site:

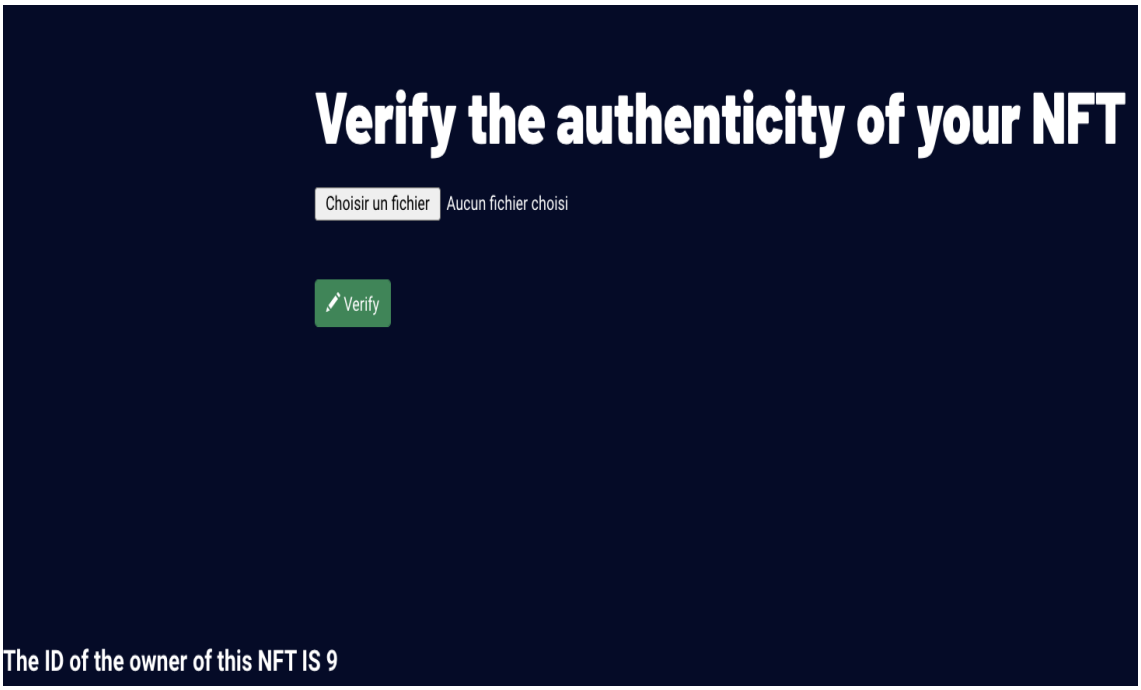
Sign in page:



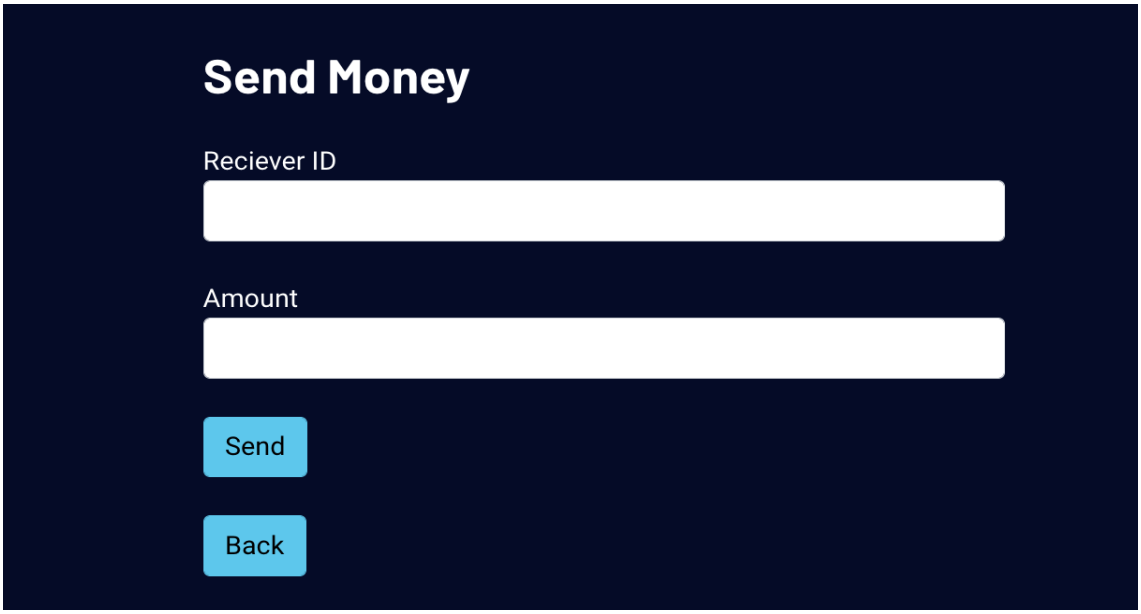
The case where the NFT is not registered (doesn't exist on the blockchain):



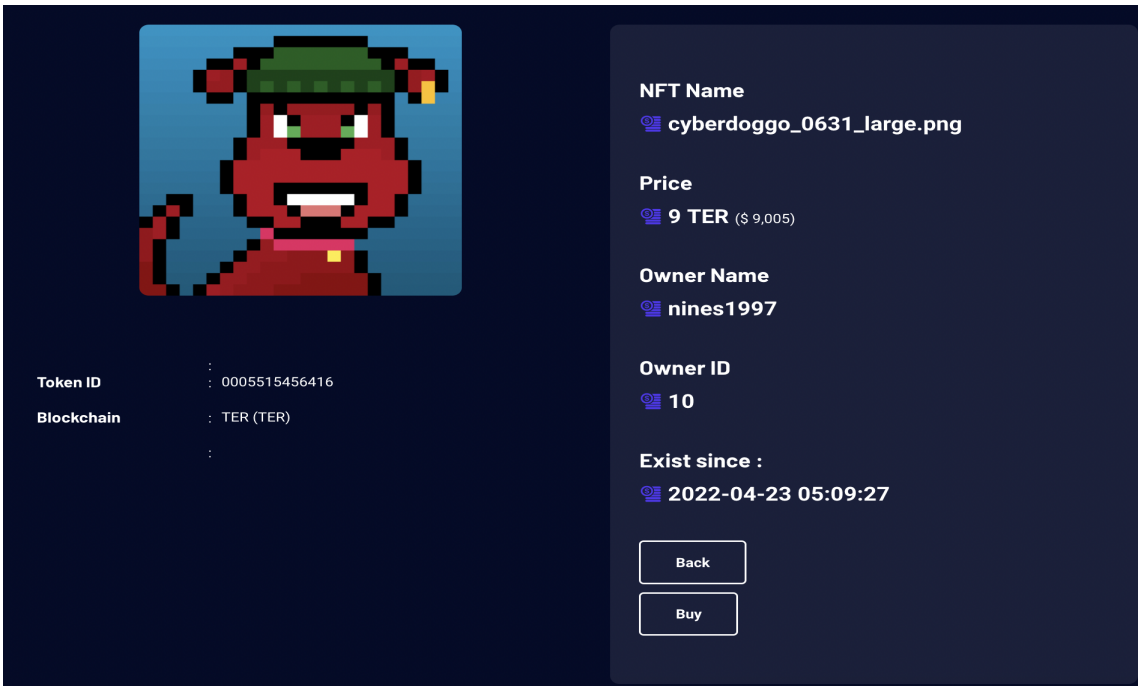
The case where the NFT is registered:



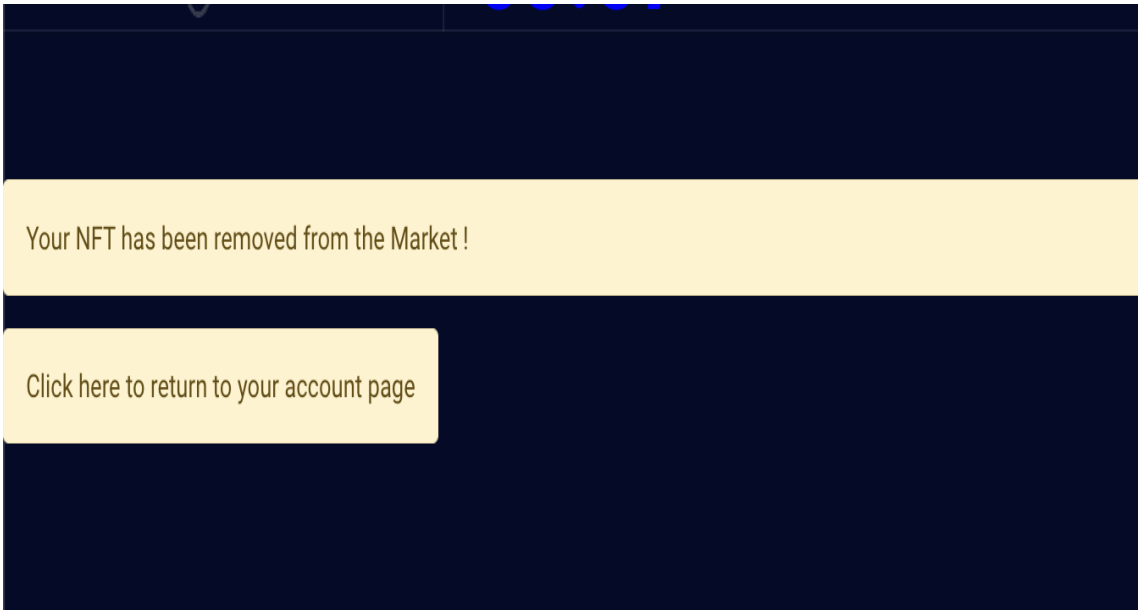
Send money form:



Description of an NFT and possibility to buy it:



Confirmation that the NFT is no longer visible on the market (hide option):



Confirmation that the NFT is visible on the market (reveal option):