

HOW TO NFT?

Chapter 2: Actions

SEPARATE SIGNALS FROM NOISE

NAVIGATE THE NFT MARKETS WITH CONFIDENCE



NonFungible.com

FOREWORDS

Arriving in the world of NFTs, we very quickly realize the technical aspect can be a blocking barrier of entry.

Many questions quickly emerge "how do I get my first NFT?" or "what is a wallet?" and it's for this reason we wanted to share with you this series and theoretical guide on the fundamentals of cryptocurrencies, blockchain, tokens and methods to understand how to analyze market trends.

We hope that in this way, access to the crypto universe and, more particularly the Non-Fungible Token universe, will become easier for you to navigate and allow you to approach the ecosystem without fear.

Initially intended to be a single manual divided into several chapters, we have decided to divide each chapter into separate manuals. Although we do recommend starting with the first volume and reading them in order, but by creating separate manuals it should also be easier for more experienced users to look for specific information.

Below is the order in which the chapters were written:

- 1) Basic Knowledge
- 2) Actions
- 3) Buying and selling NFT
- 4) NFT Universe
- 5) Analytics
- 6) DeFi x NFT

We wish you a pleasant reading,

The NonFungible Team



SUMMARY

| | |
|--|-----------|
| Forewords | 2 |
| 1 Wallet Type and Usage | 5 |
| 2 Signing and authentication | 9 |
| 3 Transactions | 13 |
| 4 Fees | 19 |
| 5 Buying and selling cryptocurrencies | 26 |
| 6 Minting NFT | 35 |
| 7 Lending and borrowing | 38 |



YOUR GO-TO SOURCE TO NAVIGATE THE NFT MARKET SECURELY

Since the start of 2018, NonFungible.com has been the benchmark for NFT Market Analysis and the only platform to offer real-time tracking of nearly 150 projects.

Explore market and discover projects

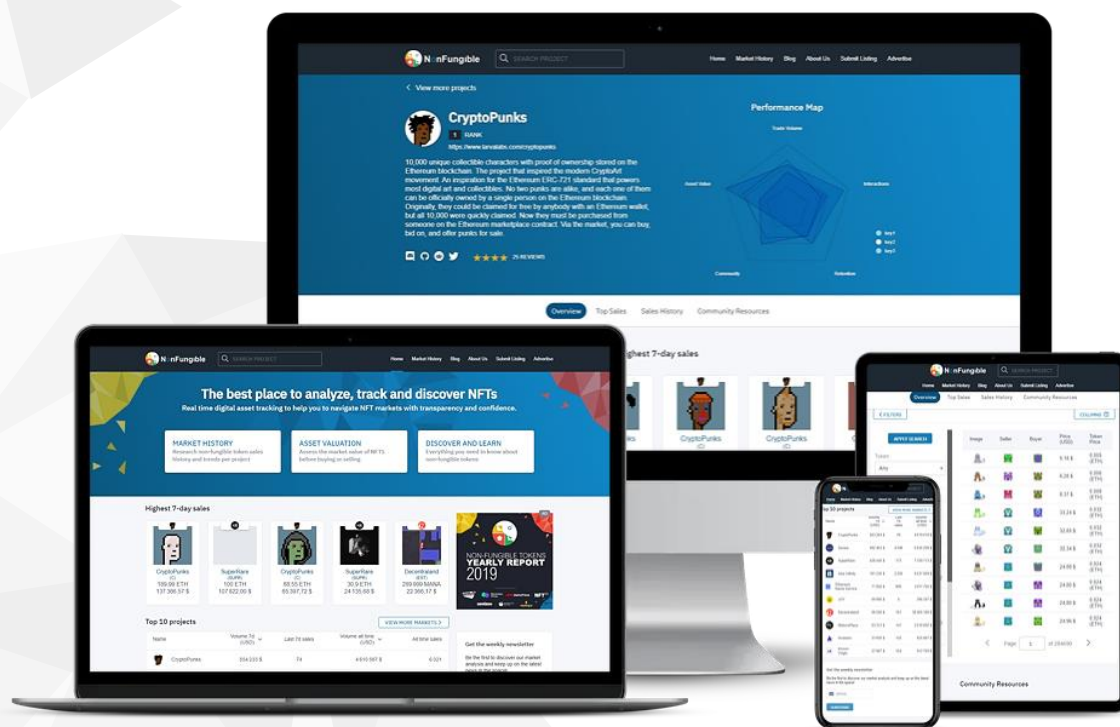
Do you want to understand the trends? Which segment performs best or projects that generate the most volume or even which Crypto-game has the biggest community?

Whether you are an experienced trader or just curious to discover new projects, here you will find all the resources necessary to enjoy your NFT journey!

Value your assets!

With real-time sales tracking, you can track the rating of any asset, find the average price of tokens comparable to those in your portfolio, or easily research before buying your next Collectible.

Don't be fooled by over-speculation, buy knowingly thanks to the market history of NonFungible.com



1 WALLET TYPE AND USAGE



One of the essential tools to be able to manipulate cryptocurrencies or their token is a wallet. Without it, your address would not exist and therefore it would be impossible to send or receive transactions.

Depending on the choice of the blockchain, the method to generate addresses will vary but the basic concept remains the same for all wallets: to be able to send a transaction to a recipient in a peer-to-peer and decentralised manner.

It is important to clarify a few concepts beforehand:

- Each address is unique
- Each wallet can generate as many addresses as you want

The number of portfolios is so large that today we can classify them in different categories, still in this issue of respecting the blockchain trilemma.

Private and Public Key, Seed Phrase

The cornerstone of any good crypto wallet is in what is known as private and public keys. Indeed, it is thanks to them that sending and receiving assets is possible.



The public key is utilised to be openly shared with others to receive assets into your wallet. It takes the form of a sequence of characters (human readable or not) that anyone will be able to view by looking for it in a block explorer.



The private key has a double use: To enable you to send funds out but also to be able to import them into a new wallet. For these reasons, it is essential to keep your private keys as secret as possible from prying eyes.

It takes the form of a series of non "human readable" characters and can be password protected.

In addition to the private key, there may be another way to recover your funds: the seed phrase. This series of 12 or 24 words has the advantage of being secure (the last word is generated randomly based on all the preceding ones) and more easily stored than a private key.



Custodial



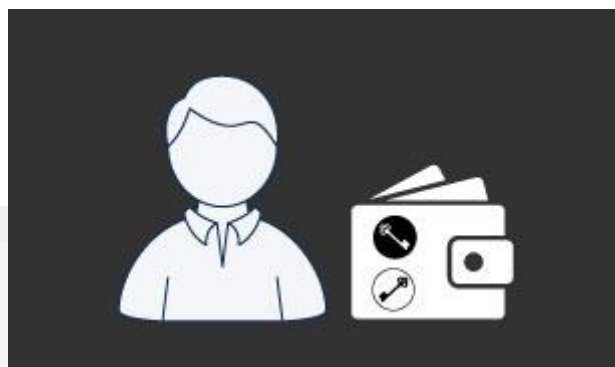
"Custodial" type wallets make interacting with the blockchain as easy as possible for the end user by generating and/or keeping the private keys of the wallets for you. In this way, sending transactions as well as any follow-up wallet interaction is technically managed by a third-party service.

The downside to this type of wallet is the ultimate lack of control over your funds as most Custodial wallets are fully configured and controlled by centralized providers.

It is important to stress that with these wallets the security of your data is not under your direct control and that if there are any issues with your funds, it will be the responsibility of the third-party service to return them to you.

Example : Argent, Revolut, Wallet of Satoshi, all these are portfolios of centralized exchanges.

Non-Custodial



Unlike Custodial wallets, the role of Non-Custodial wallets is to put the user at the center of security policy. As soon as the address is created, the secret key or seed phrase is given to the user and is generated without the wallets developers intervening.

It is therefore normally impossible for the developers of a Non-Custodial wallet to be able to locate a lost private key or seed phrase!

Example: Wasabi, Metamask, imToken, TokenPocket...



Hot & Cold wallet



In addition to the Custodial or non-custodial classification that determines “who generates the private keys”, there is a second classification, that of “hot” or “cold” wallets.

These terms are used to identify if the wallet has been designed to be permanently connected to the internet or if its purpose is to remain offline to increase its level of security.

Depending on the use to be made of the wallet, one will be privileged over the other:

- **Hot wallet** : for frequent use this can be a web browser plugin or a smartphone app
- **Cold Wallet** : for occasional use, can be a sheet of paper or a USB device

Generally, cold wallets are used to store large amounts of money or rare assets. Indeed, the movement of the assets requiring a physical action of the owner in the real world, that makes hackings of this type of wallet almost impossible.

Hot Wallets are much easier and faster to use, but they have the disadvantage of being more exposed to hack and phishing risks. This can take the form of malware while installing the wallet or more sneakily replacing the address in the clipboard at the time of a transaction.

Examples of Cold Wallet : Ledger, Trezor...

Examples of Hot Wallet : Metamask, Tronlink, Wallet of Satoshi



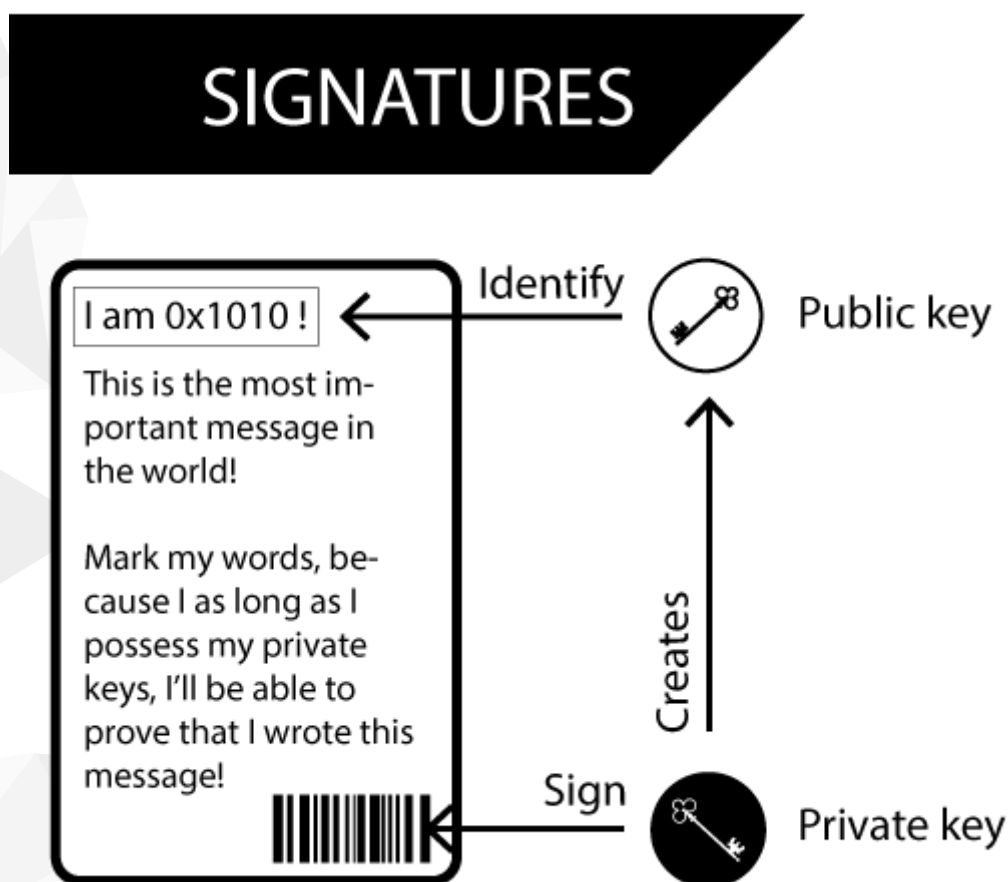
2 SIGNING AND AUTHENTICATION



Blockchain isn't just for sending assets from one wallet to another, it can also be used to digitally sign something. It can be a document but also authentication on a website for example!

This technique has been used since the 1970s, notably thanks to Public Key Cryptography (PKC) technology, which allows a recipient to verify the signature of a private key using the public key.

It is important to specify here that the process which encrypts a signature can be independent of the blockchain and the Internet, as long as the public key is known it is possible to recognize whether it is indeed it who has digitally signed an action (messages , documents, transaction...).

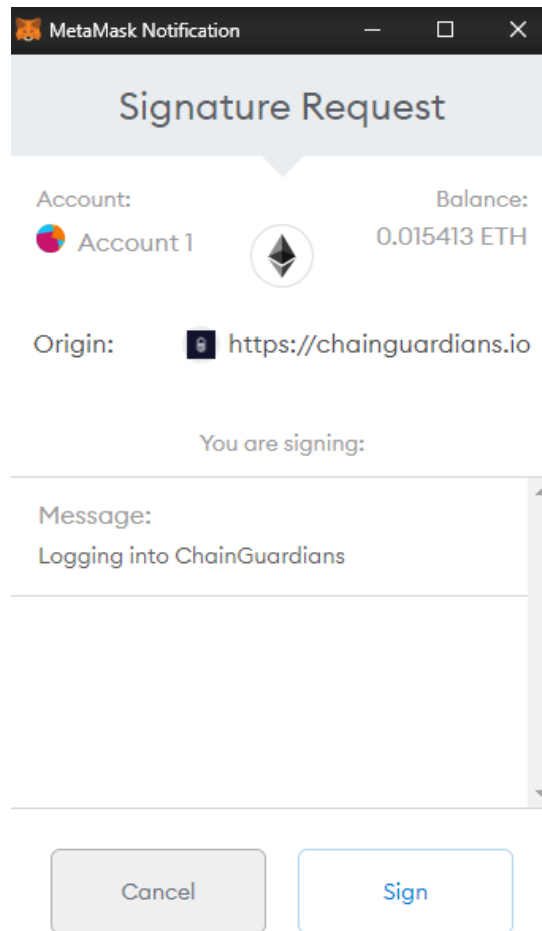


Concretely, on the blockchain, the role of the PKC is to ensure that only a supposedly legitimate owner of the funds will be able to sign a transaction to create a transaction.

For example, if Craig Wright were really Satoshi Nakamoto, he would be able to digitally sign a message using his private keys from the wallet of the person behind Bitcoin ...

Thanks to Web3 and Decentralized Applications (dApps), this method of online authentication has become very popular in the crypto space!

Thanks to a simple browser plugin, the link between the public key and the private key of the wallet can be proven and therefore allow access to the desired site in this way.

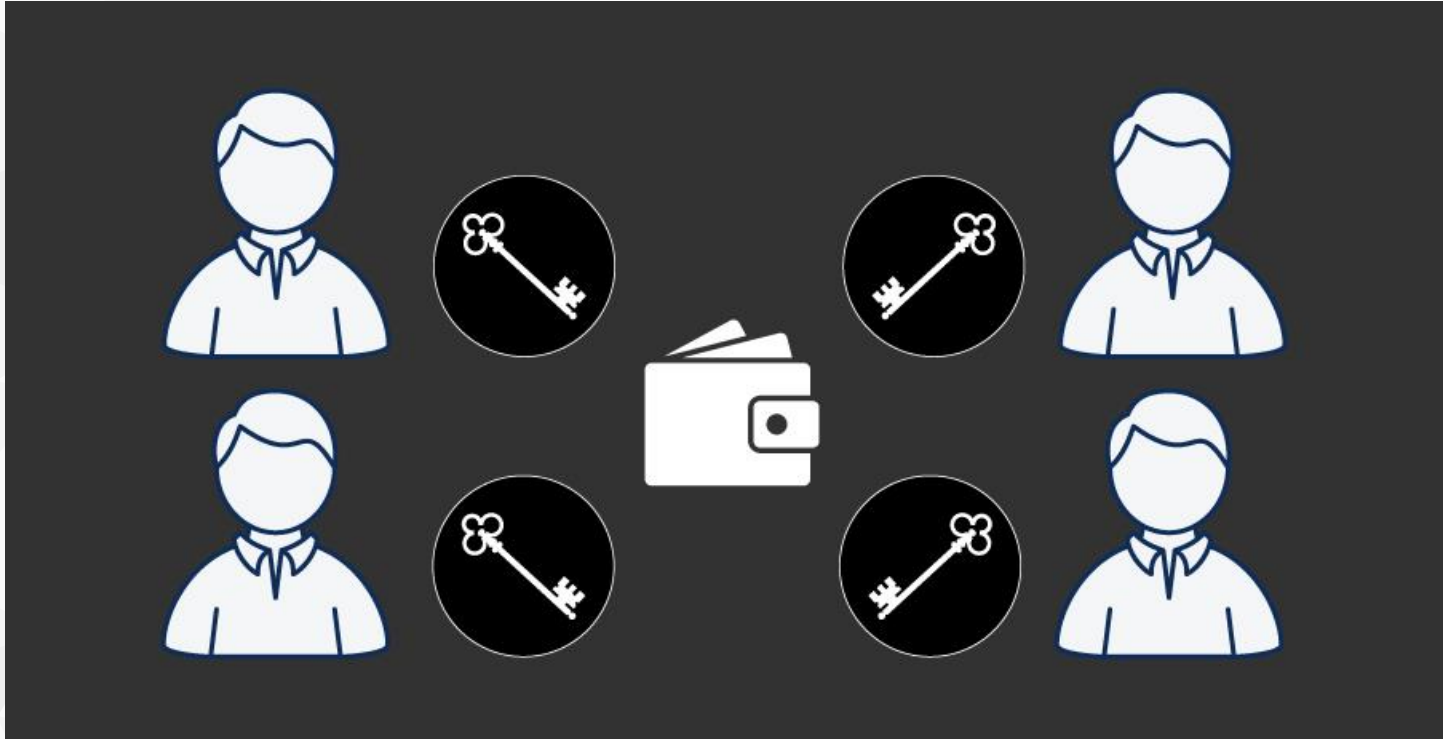


Thanks to this digital signature, even if access to the account by username and password was compromised, the third party could not move the funds in the wallet.

In the next chapter, we will see transactions on the blockchain and how the signature plays a major role in sending transactions.



Multisignatures



Another use of signatures, commonly called “multisig” is a method that allows you to have a required number of signatures from several private keys before the information is verified!

This method is one of the most secure to access the contents of a wallet, but its weak point also lies in its strength: it is enough that one of the parties is unable to sign (has passed away, are in prison ...) for it to be impossible to move the funds!

3 **TRANSACTIONS**



Now that we know how a digital signature works and especially how it interacts with the blockchain, there are still a few things to learn before sending your precious cryptocurrencies to a recipient.

The digital signature is not the only action before a transaction can actually be written to the blockchain. Indeed, the information to be transmitted by the blockchain will be "hashed". In other words, be transformed into a series of characters which all have the particularity of weighing the same weight!

Once this is done, the digital signature takes place to prove that an identity has indeed created the information that is to be transmitted..and then leaves room for the verification. The blockchain was designed so that it is possible to verify the public information but with the least possible level of trust required from other verifiers.

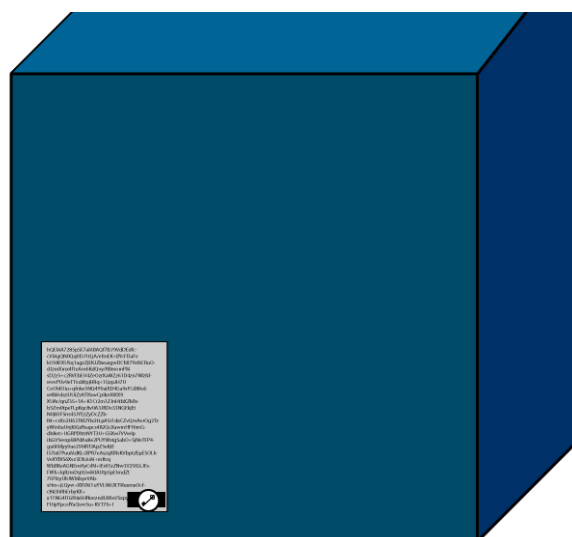
Birth of a blockchain transaction



HASHING



SIGNING



VERIFY

Depending on the choice of blockchain, the transactions do not all work in the same way, but nevertheless, are based on the same concept:

Transfer value in the most decentralized and safest way possible.

The chapter dedicated to Mining enters into more detail about the different transaction verification processes, here we look at differentiating between simple and complex transactions.



Simple transaction



What is called a “simple” transaction is a transfer of cryptocurrency from one wallet to another. This is the easiest operation for the network to perform because it only requires debiting one wallet to credit another.

Once the transaction has been signed with my private key, the blockchain will be consulted to see if I have the funds and then the transaction will be sent on to the miners so they can execute it.

Because of its simplicity, this type of transaction is the least expensive in terms of fees, regardless of the blockchain used!

Complex transactions



As the name suggests, a complex transaction is..more complex! Some features enabled by the blockchain allow for more sophisticated operations than simply sending crypto from one wallet to another. This is made possible in particular thanks to the use of smart-contracts which automate all processes.

As each of the blockchains use a different operation to make the smart contract work (Script for Bitcoin, EVM for Ethereum...) in order to remain as clear as possible, we will list here the most common use cases of so-called complex transactions.

Sending (non)Fungible Tokens

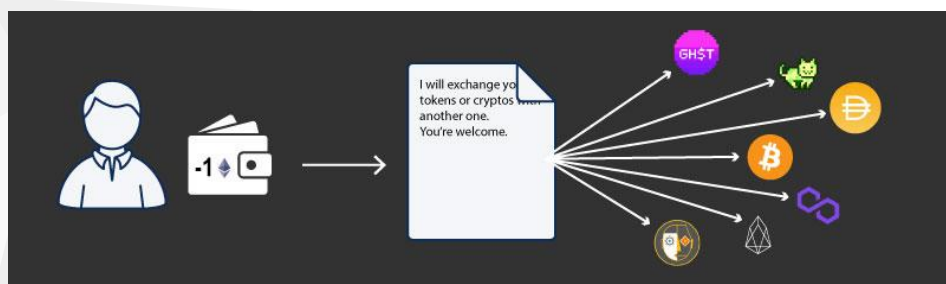


As we have seen previously, a token is a token that is linked to a cryptocurrency. This means that unlike a crypto where the blockchain was designed to natively support transactions for its currency, tokens must necessarily go through a smart contract to be able to transit from one wallet to another.

To take the example of the Ethereum blockchain, this is why sending \$MANA from one wallet to another will always cost more in fees than just sending Ether: miners will have to read more lines of code to complete the transaction and that is why the "gas limit" is higher. Likewise, sending an NFT will call a smart contract containing even more lines of code and will therefore cost even more!

This system of reading a line of code by miners or validators is the same regardless of the blockchain used. Even though in a PoS system the fee system is different, the complexity of sending the transaction remains the same and will therefore require more time for the validators on the network to complete the transaction.

Atomic and Token Swap



To be able to exchange one cryptocurrency for another (BTC for ETH for example), it is possible to do in a completely automated way, this operation is called an Atomic Swap.

Some decentralized exchanges like Bisq allow this, but it is a very complex operation and above all very frowned upon by regulators.

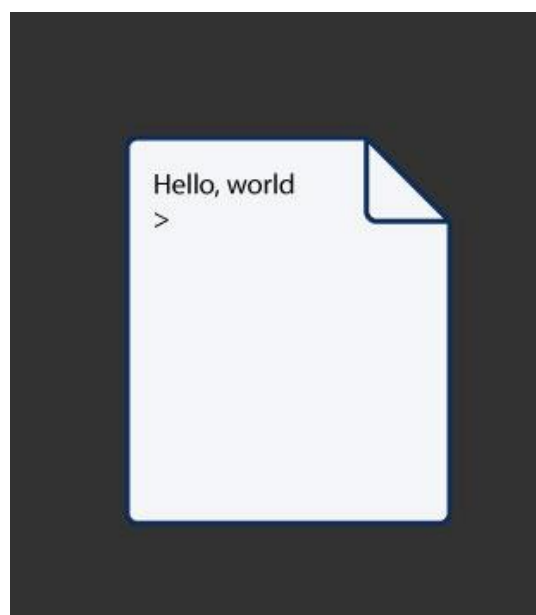
This requires having sufficient liquidity in the market on one hand, but also absolutely flawless security to avoid hacks on the other!



Atomic swaps are therefore mainly carried out on centralized exchange platforms, but it's important to know that between what is displayed in real time in your portfolio and the "concrete" realization of the atomic swap, it can sometimes take place quite a long time! This arbitrage allows time for exchanges to ensure they are trading at the best possible price, but not for you, for them..!

The token swap uses roughly the same principles as the atomic swap except that it takes place on the same blockchain. Thanks to the use of a standard understood by all smart contracts, this greatly facilitates the management of the process and the exchange between two tokens is much easier. Although it is possible to carry out tokens swaps in a decentralized manner, notably thanks to Uniswap or directly from Metamask, this can sometimes be very expensive in transaction fees!

Creating a smart contract



Among the most expensive operations to perform is the creation of a smart contract. Indeed, to be able to create what will be the automation of an entire process, it is necessary to include all the code in a transaction that is needed for the operations you want to trigger to register it to the blockchain.

There are two possible solutions to create a smart contract:

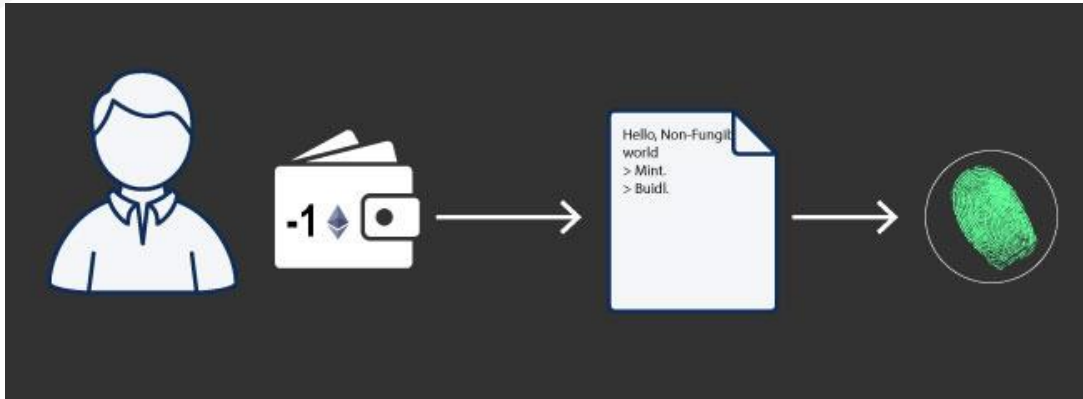
- Write everything from A to Z and then deploy it on the blockchain where it will be verified.
- Use a smart contract that will create yours

The first solution obviously allows almost total freedom of creation (depending on the ability of the blockchain to process the contract) but requires technical skills that are not within everyone's grasp.

However, there are many resources available on relevant sites and existing communities are very helpful towards new developers who want to get started in the creation of smart contracts!



NFT Minting



Among the functionalities allowed by the creation of a smart contract is the birth of an NFT or 'minting'. Minting an NFT requires sending a certain amount of information to the smart contract which then allows this unique token to be created on the blockchain and above all, deliver it back to you.

As we saw above, sending a token is already relatively expensive in gas, here the operation is even more tedious:

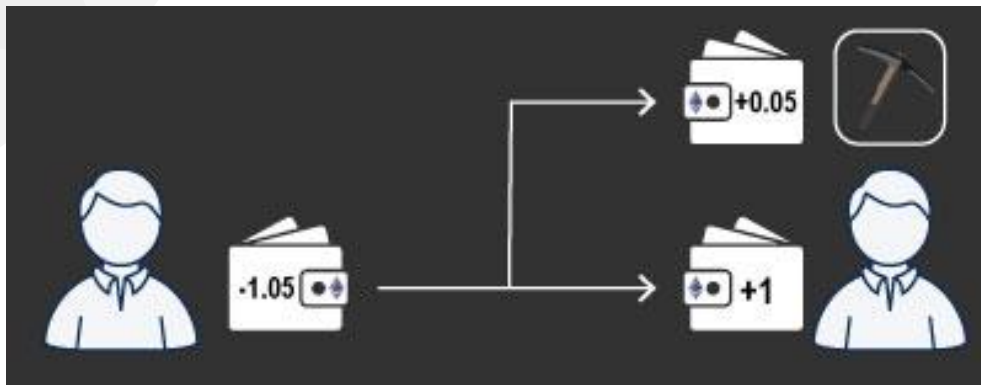
1. Send the metadata relating to the NFT to create (called image, owner, number of editions, etc.) to the smart contract
2. Execution of the smart contract to create the desired NFT
3. Issue the NFT to the owner

It is for this reason that creating your own collection, for example on Wax, Opensea or Rarible, can be expensive and time consuming: you must first create a smart contract and then mine an NFT to sell it!

Some platforms like Makersplace, Known Origin and SuperRare having already created the smart contract beforehand, the user only has to mint the NFT and wait before being able to put it up for sale.

4 FEES





As we have seen previously, depending on the consensus used by a blockchain, a fee will be charged to send a transaction. Each consensus has its advantages and disadvantages, always responding to a balance between security, scalability and decentralization.

These costs seem restrictive at first glance but if we take a closer look, they are essential! Even if they take many forms, their function is primarily to secure the network to avoid the disliked "double transaction".

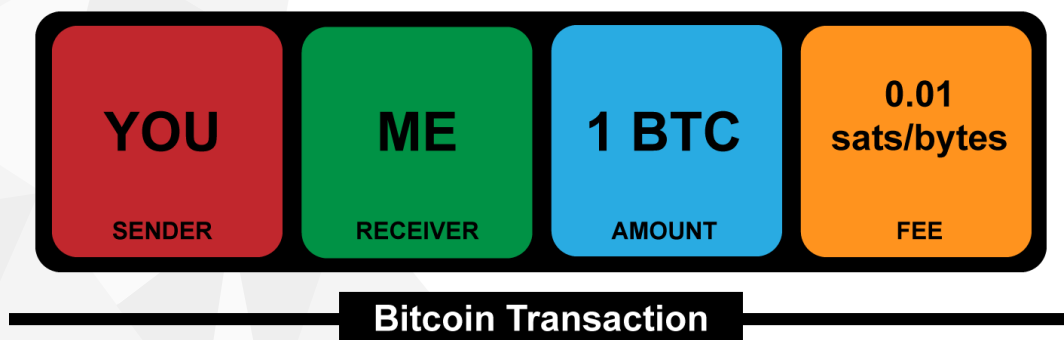
Depending on which blockchain, fees can be used to reward the miners for being benevolent towards the network but also become completely invisible to the end user in order to facilitate various uses.

Bitcoin

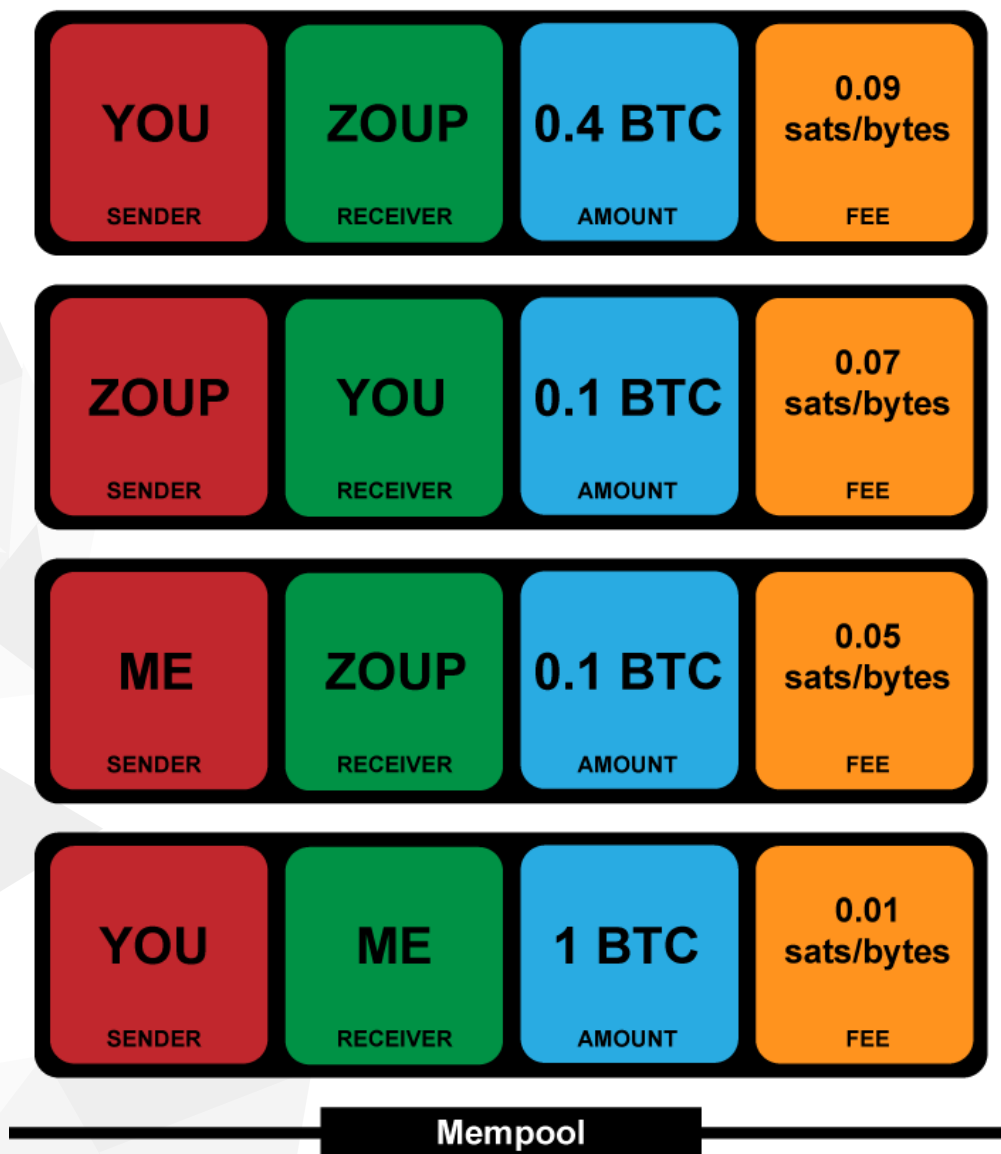
To understand transaction fees on the Bitcoin blockchain, you must be aware that each transaction is processed one after the other by miners with a proof of work consensus.

Depending on the length of this "queue", called 'Mempool', your transactions will take more or less time to be validated!

This is one of the big drawbacks of the Bitcoin blockchain: if there are too many transactions on it, it could take several hours or even several days before the transaction is put in a block before being broadcast on the network!



The fees are expressed in satoshi/byte and are calculated based on the length of the transaction. So called 'long transactions' will, for example, be a transaction to several recipients... but even if most wallets nowadays pay these fees according to the queue, it is possible to pay more for your transaction to make it a priority over others.



As explained above, miners take care of entering the transactions into blocks, but not just in any way. Since fees are a form of payment for them, they prioritize transactions with the most fees.

In the diagram above, the transactions will therefore be processed by the miners from top to bottom.



Second Layer: Lightning Network



Thanks to smart contracts on Bitcoin, it is possible to **open a bidirectional channel** on the network, more commonly called "micropayment channels". This payment channel will be reserved for two entities and must be supplied with Bitcoin by both parties wishing to use it.

Let's take an example :

Zoup and Dan want to play poker. Each one puts 1 Bitcoin in this channel and divides the 2 Bitcoin into 1 million satoshis each. They will not be able to trade more than 2 million satoshis during the game.

*They will be able to carry out a very large number of transactions and in order to keep the accounts Dan and Zoup will need to complete an **engagement transaction** from time to time which marks a "milestone" in the exchanges.*

*Once the poker is over, Zoup and Dan will only have to **close the channel** to receive the Bitcoin owed to them.*

Being able to use the Lightning Network is not free: When the channel opens, during engagement transactions, and when the channel is closed, Bitcoin's usual transaction fees revert. Also, each transaction carried out in the channel costs 1 Satoshi.

Having the ability to open up "micropayment channels" has enabled video game use cases to instantly reward gamers in satoshis much faster and much cheaper.

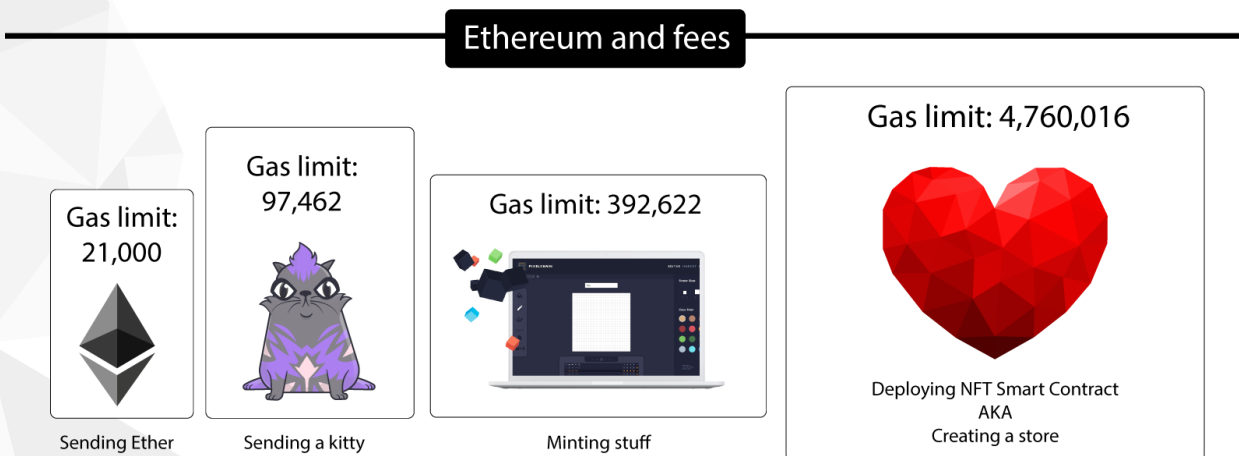


Ethereum

Ethereum also uses Proof of Work as a consensus, its way of handling transactions' rewards is very similar to Bitcoin. Each transaction must be entered into a block by the miners to be confirmed and the fees serve both to secure the network and to reward the miners.

Transaction fees are paid in Gwei and are commonly called gas but behind this name are two concepts: the gas limit and the gas price. To determine the final price for transaction fees, simply multiply the gas limit by the gas price.

Even if the calculation seems simple at first glance, it is important to know that the gas limit varies according to the type of transactions that will be carried out. Between sending Ether to a friend or deploying a smart contract there is going to be a very important difference!



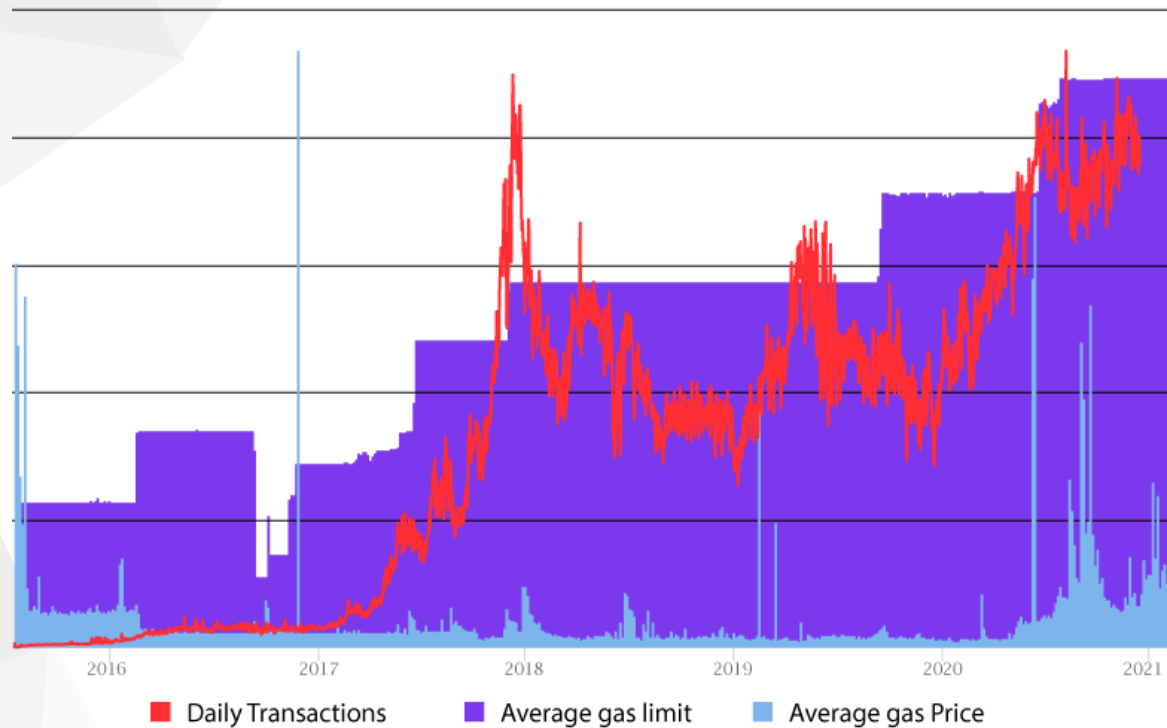
This is how Ethereum works: the more lines of code there are to read and validate by miners, the higher the gas limit will be. The limit referred to in “gas limit” is the minimum limit for the entire code to be read and validated by miners.

Regarding the maximum limit, it is determined by the storage capacity of a block, namely 16,000,000 of Gas. Since August 2021 and a major network upgrade (EIP-1559), the storage capacity has become dynamic.

To put it simply: as soon as the block is filled with more than 10,000,000 of gas, the size of the next block is adjusted, up to a total limit of 16,000,000 of gas.

Once this maximum is reached, you have to wait for the next block to register the transaction.





The price of gas balances according to the use of the network. You might think that the more trades there are, the more the price increases, but as the graph above shows, this is not always the case.

Although between 2018 and 2019, the use of NFTs experienced a slight increase, 2020 was marked by the arrival in this ecosystem of institutional actors as well as the creation of numerous digital creations. Besides that, the possibilities offered by the DeFi sector have also been very successful!

EIP-1159

Since the transition to EIP-1559, the transaction system has changed. While before August 2021 it was enough to pay the gas price to send a transaction, but now there is the Base Fee..

This base fee already existed before but was managed by the miners. Now, it is the user who can control it depending on the congestion of the network.

It is also important to understand that now the fees are no longer redistributed to the miners but are burned. The EIP-1159 is therefore the stage where Ethereum becomes deflationary.

The next step will be ETH2 and the transition to Proof of Stake!

Second layer: Polygon (ex-MATIC)

This overlay has an extremely simple goal: to radically lower the costs as well as the time of Ethereum blockchain transactions. Designed above all to facilitate the exchanges of the ERC-20 and ERC-721 standards, it is nevertheless necessary to pass through a “bridge” between the Ethereum blockchain and the Polygon overlay so that the assets can be transferred.

Unlike the Lightning Network where it is necessary to close the channel or send an engagement transaction for the exchanges to be registered on the main blockchain, it is possible to see the transactions taking place on Polygon publicly.

For transactions to be validated, this secondary blockchain operates as a Proof of Stake system, which requires a minimum number of tokens to be able to participate in securing the network. As a result, the costs inherent in the transactions are therefore a reward for the various users who have staked their tokens.

EOS and WAX

The fees on WAX and EOS have nothing to do with the previous examples. Both based on the EOSIO protocol, they use the same way of operating for the management of transaction fees. This protocol works in Delegated Proof of Stake and in order to work it requires having frozen resources in the wallet.

Depending on the dApp you want to interact with, these cryptos use between three types of resources to complete the transaction: RAM, NET and CPU. On EOS, the CPU and the NET regenerate over time while the RAM will have to be redeemed after a while.

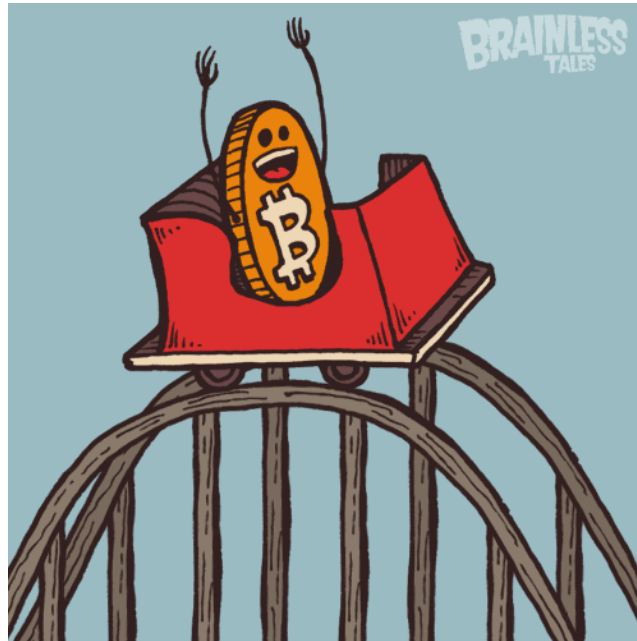
The transaction-intensive dApps quickly raise these different counters and if ever too many transactions take place on the network, a risk of congestion of another type will appear which will require stacking a gigantic number of EOS or WAX to be able to interact with the blockchain.



5 **BUYING AND SELLING CRYPTOCURRENCES**



In March 2018, John Oliver said on HBO “Cryptocurrencies are Everything You Don’t Understand about Money, Combined with Everything You Don’t Understand about Computers”. The context? Bitcoin went from \$20,000 to \$7,000 in less than a few weeks, bringing down the entire crypto market with it.



One of the key issues for cryptos is understanding what they are for and what issues they are looking to solve. Whether you are a trader, investor or just curious, here are some tips to follow BEFORE you spend a single penny in this universe:

- DYOR / Do Your Own Research: If a project sounds interesting to you, find out who the team is behind it, what they've done before and if they exist in the real world (articles, conferences..) Take time to read the Whitepaper to find out how the governance of the project works and how the cryptos or tokens are distributed.
- Don't trust, verify!: it is important not to rely solely on marketing related to a project. There are many announcements that can be misleading and verifying the information received is essential
- Don't FOMO, don't panic and bring a towel: There are many groups doing "Pump & Dump," the practice of coordinating to drive the price of a crypto up or down. Keep a cool head, establish a win-loss strategy and stick to it.
- Never EVER share your private key!!



Where to buy?

In the world of cryptocurrencies, buying and selling assets has become very easy today through centralized exchanges like Kraken, Binance, Coinbase among others. However, these platforms require having at least a blue card at best or an identity card at worst before they permit the buying or selling of cryptocurrency for fiat money.

There are peer-to-peer purchasing methods through platforms like Localbitcoin (or Localethereum) that allow you to use Paypal, a bank transfer or even according to the sellers, in cash. Crypto prices on these platforms are often higher than the market, but there are times when a seller forgets to match their prices to the market and you get a good deal.

Some projects like Bisq even want to go further by offering a decentralized exchange, but this requires a high level of technical knowledge making this solution not very accessible to the general public.

Since 2010, the possibilities to hold, transfer, buy or sell cryptocurrencies have multiplied and this has provided access to a wide variety of tools paving the way for greater adoption.

Some historical reasons to buy or sell crypto

The big question that is usually associated with the first is: why buy crypto? The overwhelming response today is “to make a profit” but that hasn't always been the case!

In the early days, cryptos were primarily technical and political experiments aimed at bypassing a traditional centralized system like banks. We saw it in the first chapters of this bible, each crypto must meet a specific need. The reasons for buying or selling must be considered and be part of a strategy, be it financial, political or even for a collection.

With individual responsibility being the way of cryptos, NonFungible.com believes that knowing their history objectively allows for a better understanding of the present situation and therefore easier to make informed decisions about the future.



Bitcoin

The early years of Bitcoin served primarily to prove that a decentralized, peer-to-peer digital asset exchange system did work.

The first crypto exchange, bitcoinmarket.com, appeared in March 2010, followed a few months later by a company that converted its *Magic: The Gathering* trading card business into a crypto exchange: MtGox. In 2011, frenchman Mark Karpelès bought MtGox and succeeded in propelling the crypto exchange No.1 worldwide in terms of volume traded.



Around this time a movement was growing within the community: Bitcoin 2.0. Aiming to seek out uses other than simply monetary exchange (such as shares, collectibles or real estate), the first ideas appear in 2012 taking advantage of the lack of fungibility of Bitcoin to be able to issue transactions by “marking” the parts sent. In a way, it was the birth of NFTs!

Their first concrete use case could be set up by J.R. Willett with the Mastercoin project which he sent the WhitePaper ('The Second Bitcoin Whitepaper') to Satoshi Nakamoto...without an answer. The goal was to be able to put in place an overlay to facilitate the use of smart contracts over the Bitcoin protocol. But with no upfront funding or time to look for it, he used the concept of colored coins to exchange Bitcoin sent to a specific address for the latter to be automatically exchanged for \$MSR. 4,740 Bitcoin financing was raised for him to carry out his project, similarly creating the first ICO in the history of crypto!

That same year, the world learned of another crypto use case during the FBI's shutdown of Silk Road, a marketplace connecting sellers and buyers of drugs, weapons, counterfeits and other illegal assets that had been in operation online since 2011. The American crypto community will defended Ross Ulbricht with all their strength in the name of the “free market” but justice remains deaf to libertarian convictions and sends Ross to spend the rest of his days in prison..

Interest in buying Bitcoin grew to exceed \$1000 in December 2013 and several central banks began to speak out primarily against its existence despite somewhat positive US opinions during the year.



From the start of January 2014 on Bitcointalk, a marketplace will change the daily life of creators around the world: [Counterparty](#) is a decentralized exchange for artists, developers or entrepreneurs using a bitcoin overlay.

Still in existence today, it has evolved over the years to provide the opportunity to create, trade, give, stake and earn dividends from artistic works in an open and free manner for anyone.



A few months later, in February 2014, a new kind of project was announced on Bitcointalk: [Huntercoin](#). Fork of Bitcoin, Huntercoin is a game and a cryptocurrency totally hosted on a blockchain! Its mechanics allow players to recover the cryptocurrency of the project simply by playing and completing quests and then exchanging them on Poloniex for Bitcoin later.

It was the first game to use the concept of "play to earn" which aims to reward players for their time spent playing rather than asking them to pay to win. Although the project was still accessible, from the start players were warned that the bots would take over one day or another.

The same month, MtGox made a sensational announcement: The company noticed that [744,408 \\$BTC](#) (around \$ 350 million at that time) was missing from its wallets and filed for bankruptcy within days. The administrative management of the company having been catastrophic, it was only when many users sold and especially wanted to withdraw their funds that MtGox realized that the daily reconciliation of the accounts had not been made for 2 years..

Thanks to the tenacity of a user of the platform wanting to recover his 12 BTC and a blockchain indexer designed by Mark Karpeles, on July 25, 2016 WME aka Alexander Vinnik was arrested in Greece by the American authorities for having stolen 630,000 BTC between 2011 and 2013 on the MtGox platform. The information is now known to all: Bitcoin transactions are not anonymous but pseudonyms.

After this shock, gradually, more and more centralized exchanges appear and despite a few hacks, going some ways in restoring the image of Bitcoin to newcomers in the ecosystem. The new exchanges become so effective that in December 2017 BTC approaches \$ 20,000 and begins a correction that will stop at \$ 3,500 a month later.





While this large drop in the market caused banks around the world to react by comparing the value of Bitcoin to the speculative folly of 17th-century tulips, it didn't stop them from seriously considering the benefits they could gain from using a blockchain!

And during this time, personalities like the Winklevoss brothers, Elon Musk and even Jack Dorsey saw in Bitcoin a real safe haven and did not fail to make it known.

In 2020, central banks are working on their closed, private blockchain CBDCs while continuing to decry Bitcoin as a technology that promotes terrorism and money laundering.

This opinion is not shared by other institutions such as Square, MicroStrategy, BlackRock or Greyscale who have bought a significant number of Bitcoin for certain whales and sometimes even at a discount by dealing with miners directly.

As of February 8, 2021, so-called “illegal” bitcoin transactions represent 0.32% of network usage. This figure is not surprising: the darknet marketplaces accepting Bitcoin have all been closed by the authorities!

Considered today as “digital gold,” the main reasons bitcoin is traded boils down to very long-term custody or trading with another cryptos for more.



Ethereum

Vitalik Buterin allegedly came up with the idea of creating Ethereum after a spell modification in World of Warcraft made his character obsolete. This need for more horizontality and transparency in decisions taken by a centralized body is strongly reminiscent of Bitcoin's response to the banking system.

In December 2013, Vitalik Buterin and seven other people founded Ethereum together by uploading the WhitePaper with two objectives: not to burden the Bitcoin blockchain and create a network of decentralized computers capable of managing applications and programs. The idea was able to charm the entrepreneur Joseph Lubin who had already been interested for a while in the concepts of cryptography and in July 2014, the 42-day presale took place with the sale of 60 million Ether for 31,591 BTC (about 18 millions of dollars).

It was in November 2015 that a technological innovation was going to be accepted by the whole community: the ERC-20. The creation of this standard would allow anyone to create their own token and therefore, a project-specific economy while taking advantage of the stability of the Ethereum network.



One of the first large-scale projects to adopt this standard is "The DAO". Each of the \$DAO tokens granted its holder voting power over the distribution of Ether contained in the smart contract.

But that was without counting two things that happened very quickly and undermined Ethereum's "code is law" philosophy: an unexpected success (\$100 million raised) followed by a 3.6 million Ether hack in June 2016.

The hacker took advantage of a security flaw in the smart contract to siphon funds from the DAO and since 45 days were needed to release the funds, he threatened to sue the Ethereum foundation if ever a fork was considered to save time.

The decision that was made at that time by 86% of the community was to rewrite the blockchain to undo the hack, resulting in a hard fork of Ethereum: the blockchain "remembering" the DAO hack was called Ethereum Classic (ETC) while the rewritten blockchain kept the name Ethereum. The hacker has never followed through on his threat!





After two soft forking of the protocol (Tangerine Whistle and Spurious Dragon) to secure the network against DoS attacks, Ethereum again inspired confidence in 2017 and enabled projects such as Bancor (a decentralized token exchange protocol) or Status (a messaging application on Ethereum, allowing both to send money and messages) to carry out their ICO.

The success of the investors was so important that the blockchain became saturated with it, rendering transactions extremely long and the network unusable.

It was in the middle of the year that the Larvalabs team had an experiment that would bring new life to projects on Ethereum. By creating 10,000 ERC-20 tokens each containing a different image of pixelated punks, the CryptoPunks were the first NFTs on this blockchain! Without any sales, it was enough to own an Ethereum wallet to claim your Punk.

But this news was only known to a few seasoned collectors because in the months that followed, a very large number of projects would launch their own ICOs until the end of the year, taking advantage of the public's enthusiasm for crypto-currencies at that time.



Yet CryptoPunks inspired what would become the standard for Non-Fungible Tokens in January 2018: the ERC-721. Thanks to the latter, it became possible to create unique and indivisible assets, paving the way for many projects, especially in the world of video games.

But due to the fall of value in the crypto markets during this period, many initiatives fall under the radar. Fortunately, this sector took advantage of its own tenacious nature to never give up, continuing to believe in the potential of ERC-721 and to proceed in creating all the tools necessary to facilitate its development:

Thanks to Metamask, a web browser is now enough to interact with the blockchain.

Thanks to OpenSea, the exchange of NFTs has taken on a decentralized dimension.

Thanks to NonFungible.com, the sales history of this thriving market became visible to everyone.

Gradually, more and more games and then art platforms appeared, multiplying the possibilities of buying and selling assets offered by Ethereum. The real difficulties encountered by this ecosystem occur during the summer of 2020 when Decentralized Finance starts attracting an increasing number of users, resulting in a new congestion of the network.

This problem, already encountered in 2017, must be resolved by the ETH2 update which began its deployment in December 2020 with the Beacon Chain update but whose impact for end users will be only a few years later. It is therefore essentially overlay solutions like Matic that make it possible to avoid excessive costs and ensure greater speed of transactions which are favored by more and more players.



6 MINTING NFTs



There are some blockchains which are programmable and are designed to allow the building of apps or otherwise known as dApps or Decentralized Applications.

Ethereum is the first and most widely used platform but there are also others such as [Cardano](#) and [EOS](#) where developers can also create and run dApps.

Minting NFTs is the term used to create the NFT from the smart-contract which is also linked to metadata, the contract has to be written conforming to certain pre-agreed standards. There are different methods of minting a Non-Fungible Token and where its metadata is stored is still of some debate.

A tokens' internal information or metadata can be either baked into the smart contract, otherwise known as 'on-chain' or the meta can be held 'off-chain' in a separate location such as a server. If you are interested in learning more about this particular aspect of NFTs please see [metadata and token attributes](#).

Writing your own smart contract and metadata is a highly skilled developer task whereas over the past few years minting on platforms such as Mintbase, OpenSea and InfiNFT among others have given creators the opportunity to simplify the entire technical process and mint their own NFTs.

This has given creators and builders the opportunity to make their own tokens when they would not have otherwise had the skills required to do so and in the process opened up the NFT Universe to an entirely new user demographic.

For example Mintbase is a global platform that allows *anyone* to create NFTs without worrying about technical complexities. Artists can create NFTs to sell digital art, musicians can use them for music, and event organizers can use them to sell tickets for their next event. Think of Mintbase as the "Shopify for NFTs". People are creating and selling [music](#), [art](#), [tickets](#), [photography](#) and much more. In a nutshell, anything other than money can be tokenized.



How to mint from a Smart Contract?

It is possible that the graphic interface delivered by the developers of a project could be malfunctioning? Fortunately, it's possible to go directly to a smart contract page on Etherscan and look for functions that allow mining directly.

Take the example of the Forgotten Runes Wizards Cult Smart Contract:

Code Read Contract Write Contract

7. isApprovedForAll

8. name

9. owner

10. ownerOf

11. price

7000000000000000000 uint256

The initial information presented is to understand price. To find this out, go to the "Read Contract" section and look for the information you want. Here the price is displayed in wei, equivalent to 0.07 ETH.

20. totalSupply

10000 uint256

To find out how many NFTs are available, look for the "Supply" section. Here we see the information that 10,000 Wizards will be available.

Now let's see how to mine directly from the smart contract, we do this in the ["Write Contract"](#) section.

14. summon

summon

payableAmount (ether)

numWizards (uint256) +

numWizards (uint256)

Write

Here the function is called "Summon" but it could very well be called "Mint". To invoke a Wizard, all you have to do is enter precisely the number of Ether (0.07 ETH for 1 Wizard) that is needed and then press "Write" for the mint to take place.



7 LENDING AND BORROWING





Lending and Borrowing within the Crypto Markets has really accelerated during 2020 with many decentralised finance platforms offering new ways to create passive income from your Crypto holdings. Cryptocurrencies have been around for over a decade and offer a decentralised peer to peer exchange of value, but monetary exchange is only one element of an entire financial ecosystem which could rival our current complex system of derivatives, options, shares etc.

Further mainstream adoption

As blockchain technology becomes increasingly accepted in the mainstream, solutions for more in depth and complex financial products and services have become more popular and trusted. It's difficult not to speak of the 2020 DeFi boom when talking of decentralised financial systems, the rapid speed at which these, mainly Ethereum, blockchain projects have grown has been mind blowing with Billions of dollars locked into DeFi platforms by the end of 2020.

Both lending and borrowing are naturally very familiar concepts with economic functions we are all accustomed to but Decentralized financial systems differ from current centralised models, one of the most obvious differences being that in a decentralised system there are no intermediaries, everything is run in the trustless peer to peer system.

No more middle man as we know them today

The middle man, for instance a loan agent or bank, is no longer required in the same way they once were, as the contract for the loan is written into the smart contract. Instead, decentralised platforms have been built that enable users to borrow and lend directly to one another.

With a simple action a borrower can access lenders worldwide at competitive rates extremely quickly, and the same is also true for lenders who can safely issue loans through a decentralised and trusted third party. Peer to peer lending and borrowing offers a much more transparent system than with non blockchain based systems, with all the transactions recorded and visible.



DeFi and NFT Finance

As Decentralised Finance gains trust and popularity the use cases for the leveraging of NFTs within this new system are also developing. The potential for Non Fungible Tokens to be used as collateral for backing loans is one element of a complex new system that is currently being formulated, for example NFTs can be utilised in the methods outlined below:

Leasing: Non-Fungible Token owners can lease out their assets to other users, leasing your ERC-721 tokens offer a way to generate passive income from your assets.

Lending: Non-Fungible Tokens holders can access liquidity by locking in their assets as collateral for loans.

Derivatives: Using NFTs as the underlying asset for a variety of derivative contracts including as a way to enable hedging investments and minimizing exposure to the price volatility of the NFT Markets.

These are just some examples but it seems extremely likely that over 2021 and beyond the inclusion of NFTs as collateral within this new financial system is inevitable as their position as unique digital assets with a verifiable value and ownership makes them perfect vehicles of value within a broader decentralised financial system. Also for NFT collectors having a way to be able to access some of that value without selling their asset is important, many owners have large sums of ETH locked up within their NFT collection.



NonFungible.com is the world's leading platform in NFT data and market analysis.

We have published this series of guides for the purpose of helping people to build a better understanding of the NFT market, offering knowledge required to develop all the tools necessary to navigate this industry.

These guides will evolve through time as the ecosystem keeps evolving day by day..

✉ contact@nonfungible.com

💻 nonfungible.com

🗨 discord.gg/nonfungible

🐦 [@nonfungibles](https://twitter.com/nonfungibles)

📷 [@nonfungiblecom](https://www.instagram.com/nonfungiblecom)



NonFungible.com