

HOW TO **NFT?**

Chapter 1: Basic Knowledge

SEPARATE SIGNAL FROM THE NOISE

NAVIGATE THE NFT MARKETS WITH CONFIDENCE



NonFungible.com

FOREWORDS

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

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

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

Initially intended to be a single manual divided into several chapters, we preferred to divide each chapter into separate manuals. Although we recommend starting with the first volume and reading them in order, this way it will be easier for more experienced users to look for more accurate information.

The following 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 What is blockchain?	5
2 What are cryptocurrencies?	10
3 What are tokens?	14
4 NFT use cases	18
5 Mining and validating	23
6 NFT and Human Mining	31



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

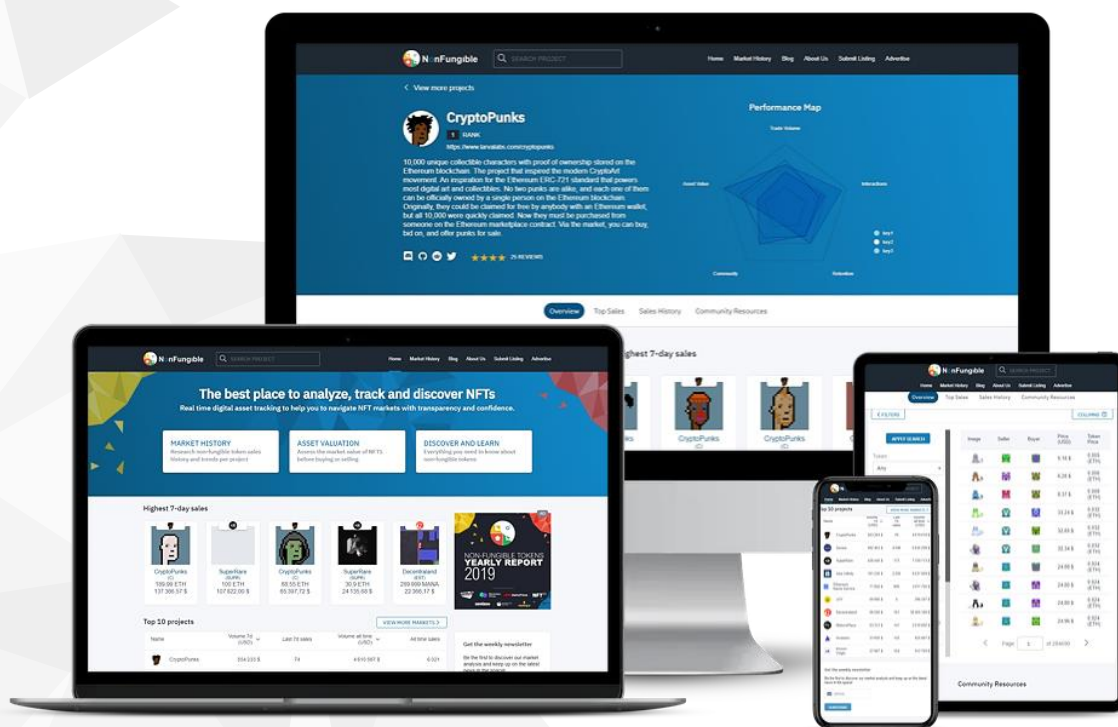
Do you want to understand the trends? Which segment performs best or projects that generate the most volume or even which Crypto-game has the biggest community?

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 WHAT IS **BLOCKCHAIN?**



INTRODUCTION

Decentralized by nature a Blockchain is based on the principle of P2P or Peer to Peer networking. The majority of these networks have no dedicated server or one single authority in control but instead function through the ongoing consensus among its user base. Becoming a user of a certain Crypto Coin or participating with a Crypto Project makes you an integral part of a greater Decentralised Network.

Blockchains are the foundation technology on which all Cryptocurrencies sit, their function ensures that each users client connected to the network can help reach mass consensus without requiring to ever trust the others.

The Blockchain is a unique type of database, there are rules on how Data can be added but once uploaded it's designed to be impossible for it to be erased, adapted or altered in any way.



This Blockchain or 'Distributed Ledger' holds Data by applying the information to individual computer files called blocks which are in turn chained together using cryptogenic technique and hash function resulting in the creation of a 'Blockchain'.

Its contents now hold immutable information with each Block carrying the DNA of the previous block as each block includes a piece of information linking back to its parent and is therefore virtually impossible to alter.



What is blockchain technology?

We've looked at what Blockchain itself is but its likely you'll have heard of Blockchain Technology, so what exactly is it?

In itself a Blockchain database is not widely usable outside of very particular applications, the exciting part is when global networks of otherwise unconnected users, developers, miners and so on develop and build communities and technologies around certain Blockchains.

In short combined with some game theory and compatible technologies a Blockchain becomes:

- A distributed digital ledger, maintained by a network of computer nodes.
- Trustless Peer to Peer Network
- Designed to be impossible to erase, adapted or altered
- Stored in cryptographic blocks

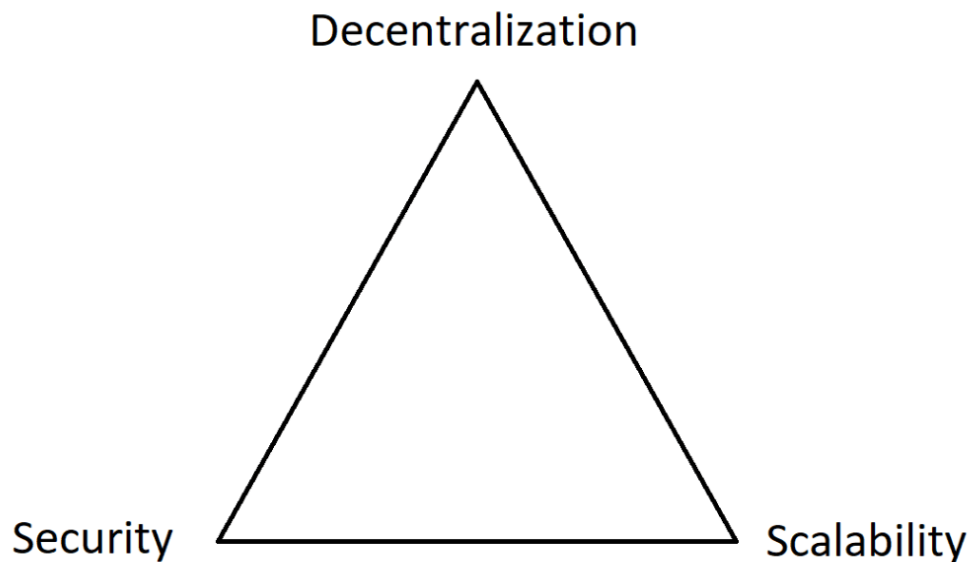
How does it work?

The purpose of a Blockchain is to ensure the flow of information from a sender to their recipient in a decentralized manner. There are several methods to get the job done, but the goal remains the same.

Governance / Protocol

Among the common attributes, first there is Governance. Indeed, the operation of a Blockchain being based on a system that does not grant any trust to its peers, it is therefore the code defined beforehand that will “make law”. Although this code will be written by developers, it is decided with other actors who will take care of running the network: validators and users.





This trilemma illustrates very well the issues to be solved when it comes to developing a blockchain:

- Decentralization represents the validators
- Security represents developers
- Scalability represents users

With more centralization, security is reduced but scalability improved.

With more decentralization, there is more security but less scalability. If it's a centric-users governance, decisions will take more time to be acted.

The use of a Blockchain must meet specific needs, therefore each one operates with its own system, which may or may not be established in a community way or not.

Consensus

Overcoming the lack of provable trust between dispersed and otherwise disconnected users worldwide is one of the main achievements of the Blockchain system, Decentralized Governance requires a trustless consensus.

Blockchain consensus algorithm is a system that permits users, both human and machine, to organise themselves in a distributed manner which in turn facilitates a secure and trustless system by ensuring that all users or 'nodes' in the system can agree on a single point of truth. These agreements will then validate the blocks and transactions, it is vital that each node maintains an identical copy of the database.

Meaning that everyone, more precisely each node, agrees on the methods used a consensus is formed around what will prove the data transfer has taken place. It ranges from solving mathematical equations by computers to delegating power to a limited number of "super validators".



Consensus Algorithms types

The only point in common between all consensus is the cryptographic aspect. If a single consensus was established between all the blockchains that would be known!

Depending on the problem to solve, several types of consensus have been thought. For example, to avoid “double spending”, it was first the Proof of Work that was applied and later the “Proof of Stake” appeared to more easily manage the number of transactions or reduce the energy impact of mining. It is important to know that many consensus algorithms were imagined long before the appearance of blockchains, but that it is thanks to them that it has been possible to implement them on a large scale!

Here is a list of the different consensus algorithms that exist today:

- Proof of Work (Bitcoin, Litecoin, Dogecoin, Ethereum)
- Proof of Stake (ETH2, Peercoin...)
- Delegated Proof of Stake (EOS, Steem, WAX, Ark, Polygon...)
- Proof of Authority (Vechain, POA...)
- Practical Byzantine Fault Tolerance (Hyperledger, Zilliqa)
- Federated Byzantine Agreement (Ripple, Stellar)
- Delegated Federated Byzantine Agreement (NEO, Phantasma...)

New types of consensus have emerged through time with a new vision of a decentralized Distributed Ledger Technologies

- Directed Acyclic Graphs (IOTA, Nano, Hedera)
- MimbleWimble
- Sidechains (Liquid, RSK...)
- Snowflakes, Snowball (Avalanche)
- Zero Knowledge protocols (Zcash, Monero, 0xZRX, Coda...)

Without going into the details of all the consensus, we are going to deal here only with the main ones, which directly or indirectly concern NFTs.



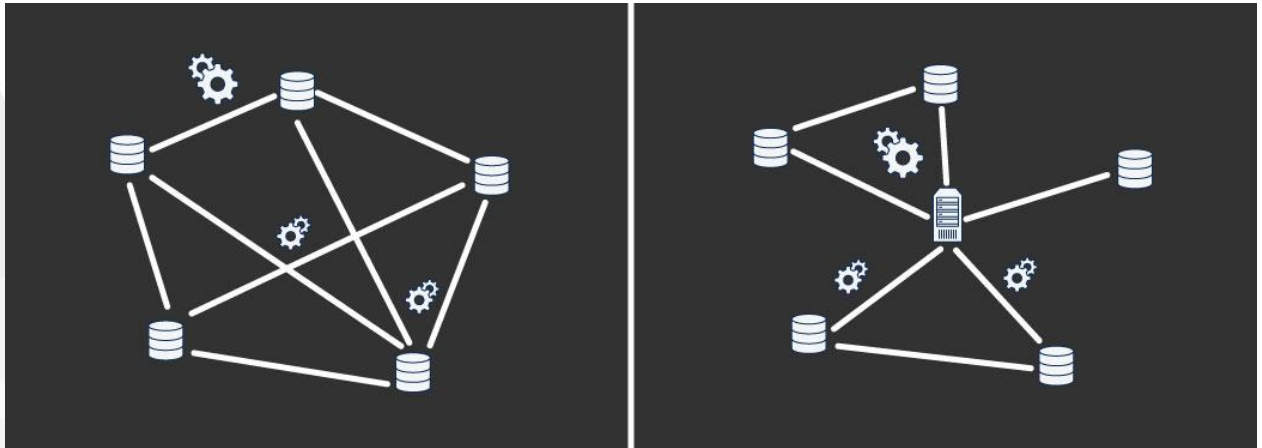
2 WHAT ARE CRYPTO?



WHAT ARE CRYPTO-CURRENCIES?

Crypto or Cryptocurrency is a digital store of value which can be exchanged and traded in the same manner as familiar global currencies. Cryptocurrency is very different from other digital solutions such as Banking Apps and PayPal, even if on the surface they might look similar and have corresponding use cases.

Decentralized vs Centralized



Traditional digital financial solutions are in essence centralised and controlled by the Governments and Companies that maintain those monetary systems. Centralized systems have a history of manipulation and interference and after the financial crash of 2007 many were looking for a more stable and fairer financial solution.

Satoshi Nakamotos' [Bitcoin Whitepaper](#), published at the end of 2008, was a groundbreaking document describing the use of cryptography as a way to create a trustless peer to peer form of electronic cash without the need for any middle party to be involved in any given transaction. The great strength of Bitcoin was above all to have been the first cryptocurrency to prevent the risk of double spending transactions.

This decentralized structure offered a potentially more balanced and equal system, with each user or 'node' connected to the network playing its part in reaching mass consensus.

Different Types of Assets

The term "cryptocurrency" includes in the collective unconscious any asset using a blockchain. Except that in reality, there are more terms to define the different categories and subcategories that exist in the crypto ecosystem.



Coins



Bitcoin



Ethereum



Monero

The term “altcoins” is used to refer to all cryptocurrencies other than Bitcoin. This is due to the dominance of the Queen Mother of cryptos which alone accounts for over 60% of the market capitalization of all crypto!

However, this term is used very implicitly and there is no specific rule that determines at what percentage a crypto becomes an alternative to Bitcoin. It is important to emphasize that each altcoin has its own blockchain.

We can therefore easily say that an altcoin is a full-fledged cryptocurrency that meets a specific need, with its community and its associated consensus.

Tokens



Polygon



Aavegotchi



Enjin

Unlike altcoins, tokens depend on cryptocurrency. They are therefore set apart from other crypto and regular confusion is made between crypto-currencies and tokens.

In order to be considered a token, they must meet a standard that allows interaction and interoperability with the blockchain to which it is attached.

It is quite common to see a project starting as a token (EOS, TRX ...) before becoming altcoin the day they decide to use their own blockchain in order to continue to evolve.



Stablecoins



Tether



DAI



USDC

Stablecoins are tokens whose particularity is to always be equal to fiat money. The oldest example of this is Tether which has been around since 2014 and which was a Bitcoin token before moving to Ethereum.

Even in times of strong demand or supply, its price has always been within a few cents of a dollar. Their utility is above all to be used for trading, allowing to make a stablecoin <> crypto exchange without having to go through the traditional fiat system.

Since the advent of DeFi, other uses have developed such as lending or borrowing stablecoin. In particular, this has made it possible to create forms of decentralized savings that are more advantageous than what a bank can offer today.

Central Bank Digital Currency

The latest creation to use a blockchain to function, Central Bank Digital Currencies are issued by the central banks of a country. They are therefore backed by the fiat currency of the country that issued it.

Unlike Stablecoins, CBDCs are issued by central banks and not by a company, foundation or association outside the fiduciary system. It is therefore a government that defines the rules for its use, emission and regulation without being obliged to ask its users what they think.

CBDCs therefore only have cryptocurrencies in name and should not be confused with all other existing projects.



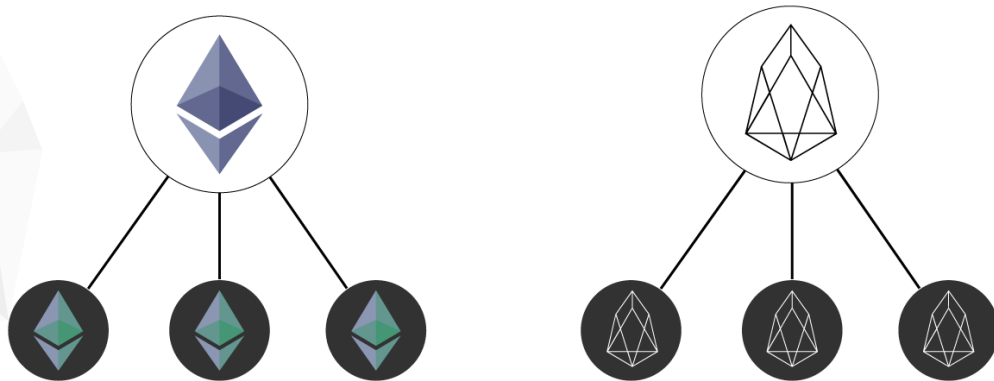
3 WHAT ARE TOKENS?



Imagine the entire Ethereum network as a vast network of 'nodes' or in other words, users computers, which are all connected together. The EVM or Ethereum Virtual Machine acts almost as a living entity, similar to the way natural organisms connect such as fungi which spreads a net of underground mycelium for thousands of miles connecting widely dispersed forests and plants.

Continuing with the analogy, if Ethereum is the mycelium connecting the forests in an underground network then Ethereum tokens and Decentralised Applications (dApps) are the trees.

Endless trees can grow in the Ethereum forest, each with their own unique properties, ecosystem and ability to seed new life.



There has always been a problem formulating true digital ownership since the days of Napster, infamous for enabling mp3 audio file sharing at the end of the 90's. They cut out the middleman and the record labels but also offered zero protection for the artists.

Finding ways for content creators and publishers to retain clear and indisputable ownership of digital media has ever since been an ongoing challenge, enter the Non-Fungible Token, each one unique and holding immutable data and proof of ownership.

A Non-Fungible token is a digital asset which has been created on top of a Blockchain, most notably held on the Ethereum network but also on other blockchain projects such as EOS, Stellar and Tron who also host Non-Fungible Tokens on chain.

Each Token is completely unique and with individual properties allocated to them, including a ledger of all activities such as its creation date, entire ownership history. Large files can also be attached and in addition, images, audio and in the near future there will be more, from full HD movies to property deeds. Each one has cross platform interoperability and can be traded on marketplaces and exchanges or used in their own environment such as in games and virtual worlds.



ONE TOKEN, DIFFERENT STANDARDS



One of the most exciting original concepts behind the Ethereum Blockchain is the ability to build decentralized applications and issue tokens on it. Since Ethereum launched others followed suit such as EOS and WAX.

To ensure that the token can be identified by all wallets and any application that wants to use it, it is necessary to create a technological standard which will be recognized in a uniform and unanimous way in the network.

Ethereum

On Ethereum, the standard that will have been recognized and voted on by the community is called Ethereum Request for Comments (ERC) and follows the Ethereum Improvement Proposals (EIP). The number following the ERC is the number of the proposal that has been submitted to the Ethereum community.

Here are the three main ones:

- ERC-20: the Fungible Token, famous for being used for Initial Coin Offerings (ICOs)
- ERC-721: the Non-Fungible Token, famous for being used by CryptoKitties
- ERC-1155: the Semi-Fungible Token, famous for achieving the mass distribution of both ERC-20 and ERC-721 in a single smart contract

To fully understand how these tokens are working, let's take a concrete example :

Zoup is playing a Role Player Game. He's going to fight the last boss of the game: the Shadow of Terror. Victorious after an epic fight, a chest appears, and he opens it. He earned 10 000 Fantasy Coins and the only Legendary Sword of Sorrow of the game.

In this example, the chest is an ERC-1155. It will be able to deliver the Legendary Sword of Sorrow (ERC-721) and the Fantasy Coins (ERC-20), the fungible token of the game.



EOS

EOS was built as a “software” to create a lot of dApps and to offer the possibility to track every transaction with a very low latency rate. So we can say that the fungible token standard is by design EOS.

A short while after its launch, a new standard was born in the EOS ecosystem: **dGoods**. This standard was made to facilitate the exchange of Non-Fungible Tokens on this blockchain but unfortunately, very few video games achieved to use it.

WAX

After its ICO early 2018 on Ethereum, Wax decided to create its own blockchain using the EOSIO ecosystem. EOSIO is the infrastructure of EOS too, but it can be duplicated to create a new blockchain based on the same technology.

The strength of the WAX blockchain is that it's designed to support NFTs with the same ease as EOS does for dApps.

FLOW

After the incredible success of CryptoKitties in 2018 that paralyzed the Ethereum blockchain, the studio Dapper Labs has started working on a new blockchain dedicated to Collectibles and gaming.

It was in 2020 that Flow Playground was born and allowed developers to create dApps on this new blockchain. By design, Flow is made to host NFTs thanks to different dedicated functions.



4 **NFT** USE-CASES



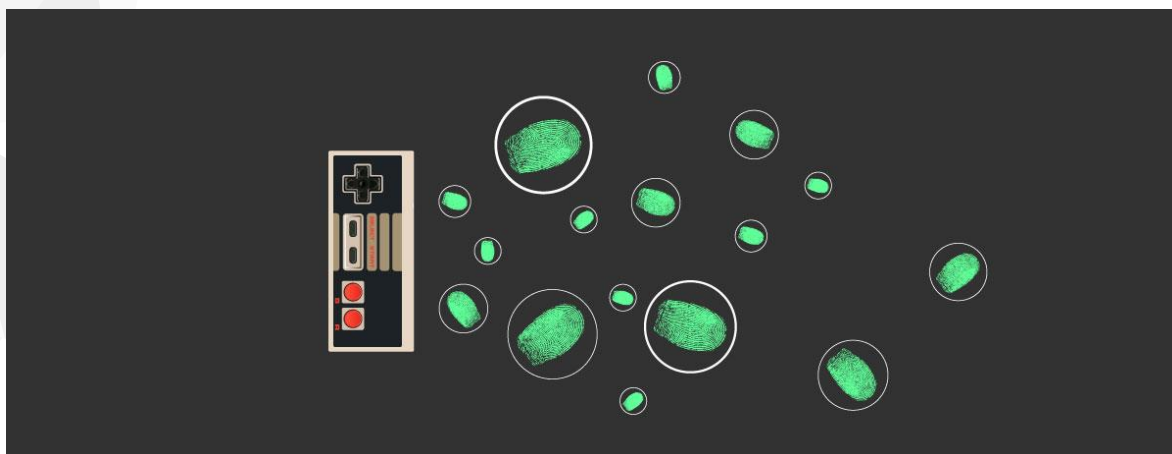
NFT USE CASES

To understand the NFT potential use cases, it's important to understand what dApps really are. Imagine playing a video game on your mobile. Each item of this game is hosted on a centralized server. Now imagine the same application using NFT as items. This application is a Decentralised Application and brings the "real ownership" to players... but there are many other use cases!

For one, there has always been a problem with digital ownership since the early internet and Napster; finding easy ways for content creators and publishers to retain clear and indisputable ownership of digital media has ever since been a challenge. The individual nature of NFTs coupled with the immutability of blockchains creates this unrivalled safety.

Non-Fungible Tokens held on blockchains such as Ethereum, Eos, Stellar and Wax have multiple use cases with many more to reveal themselves in time to come. One such example is their ability to be interoperable between different platforms and Virtual Worlds, for instance having an NFT avatar that can travel between games and be sold on multiple NFT marketplaces.

Gaming



Potentially one of the most exciting use cases for NFTs is in-game digital assets. One of the issues with Blockchain and Crypto has always been finding a path to mass adoption and NFT in-game assets seems set to be the most likely catalyst for this long-awaited moment.

Virtual economies in games have existed for years, such as marketplaces, currencies and in-game assets such as skins and weapons in games like Fortnite and World of Warcraft, but currently these are tied to each game that they are played in.

The markets in these games are largely unregulated with no real-world value except for the value placed in them by the players. The interoperability and security from having these and more held on a blockchain is immense.

NFT in-game assets have a layer of security built in and in addition can be openly traded directly for Crypto or traditional Fiat, \$£ etc, on regulated and decentralised marketplaces. Also digital ownership enables players to earn real world cash for their time and skills spent playing the games.



Governance



Is another aspect of this new digital economy as individual games issue their own NFT tokens enabling holders to vote on future developments of the game, meaning they have power within the ecosystem they use to shape the virtual world.

Also governance tokens have an economy of their own, again they can be openly traded for real world currencies, farmed or returned back to the game to add liquidity from which you earn passive income.

Art



Although digital art has existed for many years, some of the vital differences with art that is held on the blockchain is its immutable data and offers proof of ownership and origin.

Since the now iconic Crypto Punks emerged in 2017, Art has become a multimillion-dollar sector of the NFT space, Punks are 10,000 24x24 pixel art images, each of which has a set of characteristics which combine to create individual pixel artworks and have become not only possibly some of the first digital antiques of the future but also increasing in value rapidly with many artists and artist NFT platforms emerging from the Crypto Art scene since.



Decentralised Finance

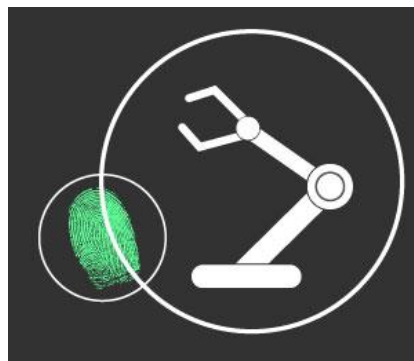


One of the more recent usecases is a merger between decentralised finance (DeFi) and the use of NFTs to achieve “DeFi gamification”. The goal of this new practice is to facilitate access to DeFi by promising very high income and very quickly even if sometimes the code is not very secure or audited.

The use of the Non-fungible Token in this part of cryptos is quite variable: it can serve as a collectible for experienced traders who have achieved good performance but also serve to increase income or receive rewards.

Since the project is focused on the DeFi and not really on the Non-Fungible Token, it is important to keep in mind that the project is high risk and therefore can cause you to lose or win money very quickly.

Internet of Things & Artificial Intelligence



Humans have always wondered what the future would be like and last century was no exception with every type of media available to us, used to visualise and fantasize about how we will evolve in the digital age.

We already live in a time where our physical realities exist in tandem with our digital personas, from banking to social media, dating, gaming and education many people's lives exist in a dual digital/physical hybrid which is only set to expand in the future. Bringing the physical, real world onto the Blockchain through tokenization is revolutionary in many aspects.

Blockchain technology brings trust, accountability into an IOT system. Non-Fungible Tokens in the ERC-721 standard can manage IoT devices and offer secure authorization and authentication for IoT devices.



Real World



In 2020 we saw more and more real-world players who started to take an interest in the potential of Non-Fungible Tokens.

The path has been paved by video games and art, but today more and more countries and companies are starting to adopt this technology for uses as diverse as they are varied:

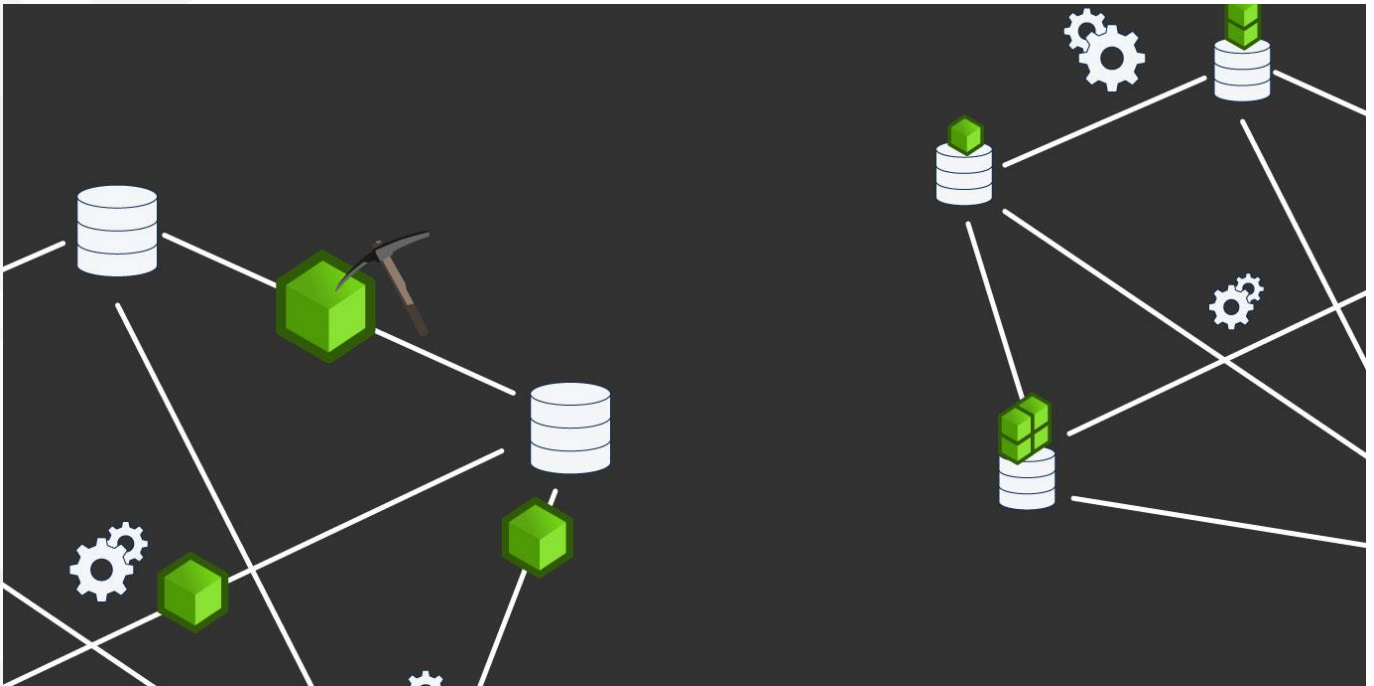
- Vietnam now delivers its diplomas thanks to [Non-Fungible Tokens on the TOMOchain blockchain](#)
- Luxurious watch brands like [Breitling](#) or [Vacheron Constantin](#) use NTFs to ensure the traceability and authenticity of certain watches
- Investing in real estate through the purchase of fractional shares thanks to the startup [Progressing Today](#)



5 MINING AND VALIDATING



MINING AND VALIDATING



Miners are one of the essential players for a crypto to work. Guarantors of the security of the network, it is they who are responsible for validating the transactions before entering them in the blocks.

Depending on the consensus (Proof of Work, Proof of Stake, etc.), their task will not be carried out in the same way but before going into the technique it is important to do a little theory.

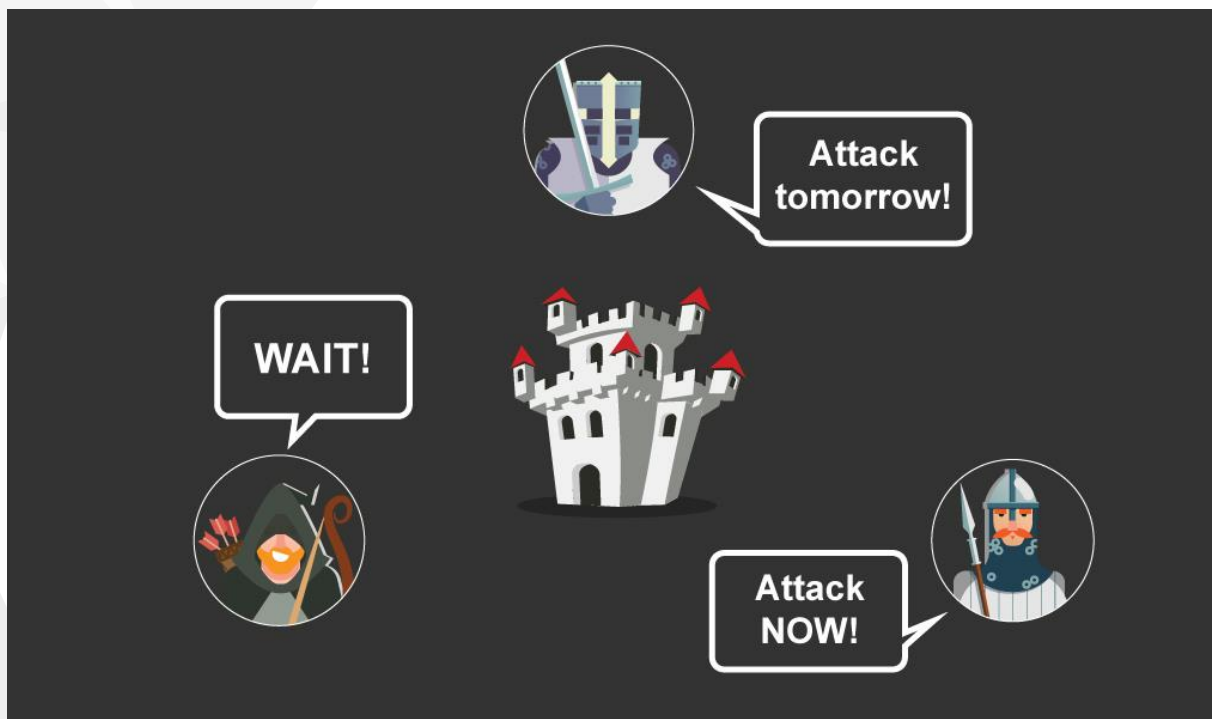
In the world of traditional banking, banks act as guarantors of transactions. Each expenditure made passes through centralized bodies that take care of the management and validation of transactions.

Having abused their position many times in the past, the trust placed in them was ruined by this behavior which had disastrous consequences on the lives of many for the benefit of a very small group of individuals.

In order to no longer leave full powers to individual entities holding too much control over the management of banking transactions, the validation of crypto transactions was first of all designed to reduce as much as possible the trust that the validators (minors, minors, etc.) could have. delegates...) in relation to each other.

To explain the problem of establishing a common strategy (consensus) between several parties not trusting each other (minors) to validate the veracity of very important information (a transaction), the metaphor of the “problem of the Byzantine generals is regularly used.





In the image above, three armies want to conquer the castle in the middle. A first problem quickly emerges: If one of the three armies attacks alone, it will be severely weakened by the attack on the castle and the other may gain the upper hand later.

By mutual agreement, the two armies decide to make an alliance but a new problem arises: When to attack? A castle spy can slip into the messengers tasked with passing information on to the other army and by falsifying the information transmitted, disrupting plans.

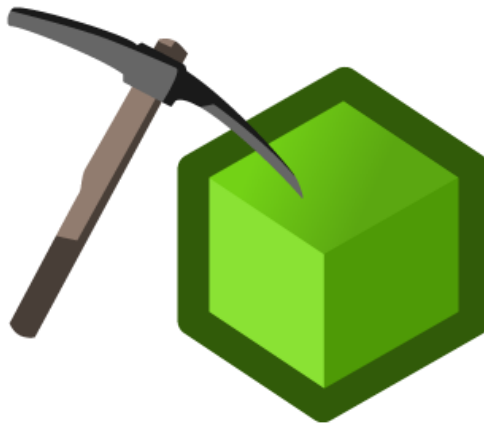
There are two known solutions to this problem:

The first is to transmit the information orally to a large number of messengers so that in this way, more than the majority of them can transmit the correct information,
The second is to transmit the information in writing to several messengers provided ... that the writing is not falsifiable.

In the world of blockchain, these two solutions blend and are combined with other methods to ensure the best possible truthfulness of information, most often in complete transparency and in a public manner.

Even if the consensus method in Bitcoin is not a majority vote, the purpose remains the same: to have a majority of validators who report the same information to be entered on the blockchain.

CRYPTO MINING



As we have seen above and in previous chapters, mining depends on the chosen consensus! Some forms are very energy-intensive but allow better decentralization while others will favor greater centralization to ensure greater speed of transactions to the detriment of security.

Sending a transaction

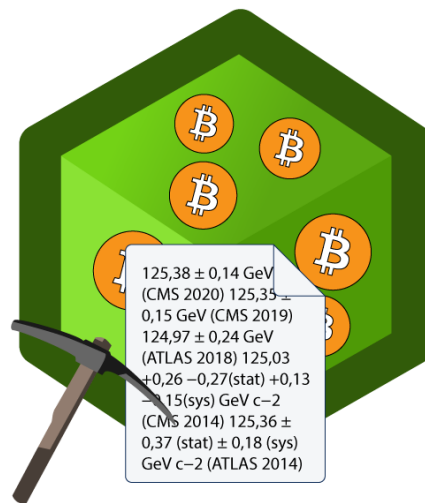
If I want to send 2 ETH to Jess, several steps will have to be taken:

1. I will “say” this information publicly by signing it with my private key
2. The nodes, which have the history of the blockchain, will check that I have the 2 ETHs in my wallet so that the transaction can be sent
3. Minors will choose my transaction if the fees are sufficient
4. They will validate that the transaction is correct by solving complex mathematical equations
5. Once the majority of miners agree on solving the math equations, the transaction is entered in a new block
6. The information contained in this block is synchronized with all the nodes of the network
7. Jess receives the 2 ETH I sent her

Minors therefore intervene in three stages of the transaction sending process: Choose my transaction, validate it and enter it in a new block. Everything else is automated in code already written on the blockchain.



Finding a new block



In this process, there is the writing of the transaction in a new block. According to the blockchain, new blocks are issued according to a defined time (every 10 minutes for Bitcoin, every 13 seconds for Ethereum...) and contain a reward which awaits the miners who “found” the block first!

For Bitcoin today the reward for each new block found is 6.25 BTC but this has not always been the case. Indeed, Bitcoin uses a method called “Halving” which halves the rewards for every 210,000 blocks mined. At first this reward was 50 BTC and once all blocks have been issued (scheduled for 2140) the only rewards for miners will be transaction fees.

For Ethereum which was thought to have massive use and not necessarily become scarce in the future, the reward per new block found has been adjusted several times over its history and will be further changed in future updates to the blockchain (ETH2).

This award attracts much envy, and it is for this reason that the miners are put into fierce competition to determine who will succeed in solving the mathematical equation contained in the new blocks first! Naturally, the miners will put more and more computing power to solve the equations first, but the more computing power there is, the more the algorithm that generates the equations will take this increase into account and the more the equations will be complex.

This balance between the computing power required to find new blocks and the generation of the complexity of the equations to be solved is called Mining Difficulty.

Mining difficulty



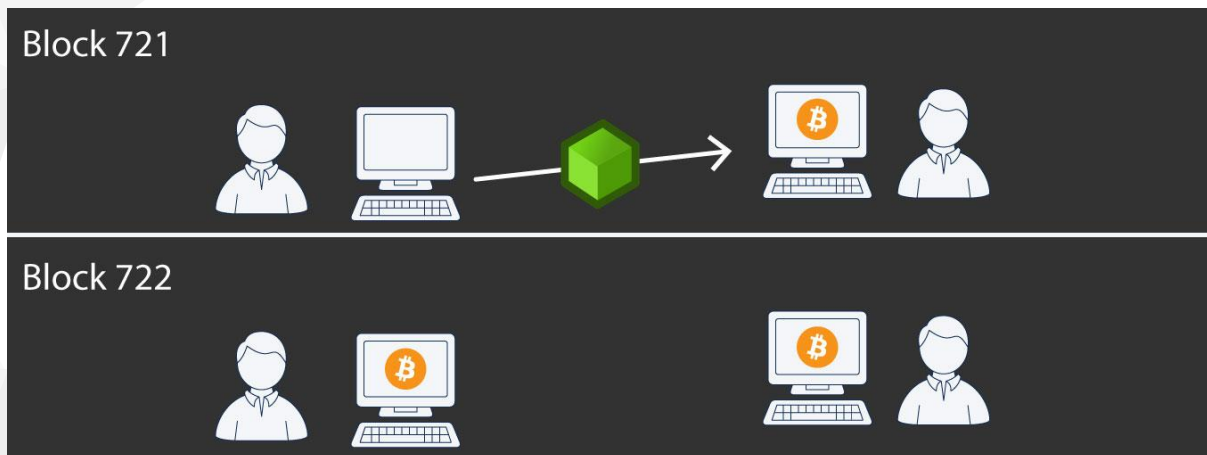
At the start of any blockchain using Proof of Work, the initial mining difficulty is relatively low because little computing power is allocated to find new blocks or validate transactions. But depending on the success of the blockchain, this will attract more and more miners who will want to participate in securing the network and in fact, it will increase the computing power and therefore the mining difficulty.

Although theoretically it is possible for a human to solve this equation by hand, using a computer tool is much faster and more efficient. At first, a simple microprocessor was enough to mine Bitcoin, then as the difficulty increased, it was the graphics card processor that was used. The next development is the use of chips that have been designed specifically to solve the equations generated by the encryption algorithm: Application-Specific Integrated Circuit (ASIC).

To further increase the probability of receiving a reward, the solution that followed was to pool the computing power of the miners in order to form “mining pools” which then distribute the block rewards and transaction fees between them. random is proportional to the computing power attributed to the pool.

You should know that some blockchains like Monero have experienced a change in the code of their blockchain (hard fork) to prevent ASICs from mining. These hard forks ensure that the mining is always provided by microprocessors and to prevent large companies holding ASIC farms from pocketing most of the rewards. .

51% attack and double spend



We have seen previously that in order to find consensus, it is essential that **more than the majority of messengers** (miners) provide the same information.

But what if the majority of miners reports corrupted information? This is the Achilles' heel of Proof of Work mining and it's called a "51% attack".

Concretely, having more than the majority of the computing power of a blockchain makes it possible to rewrite part of it (see all) and this can have several consequences, one of the most famous of which is that of double spending.

Taking the example of the transaction that I sent to Jess previously, the majority miner group will be able to erase the transaction in the next block and this will have as a direct consequence the cancellation of my debit but not the cancellation of the credit in Jess's wallet.

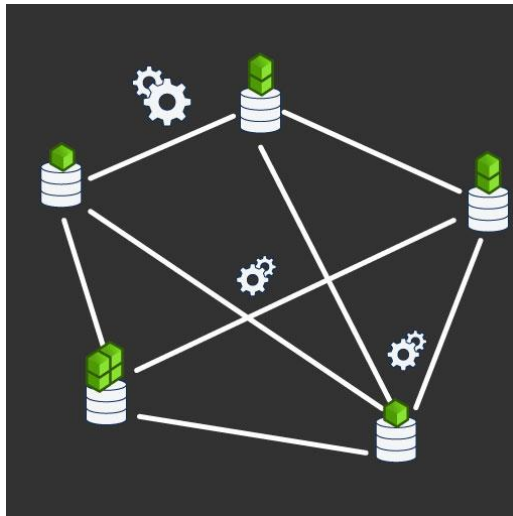
When a 51% attack is underway the majority group of miners will mine a longer blockchain on their own and synchronize with other nodes than when they want to resell. The negative effect of this method with cryptos is that it causes the price of the relevant crypto to drop almost instantly.

But since the blockchain is not only used for crypto-currencies, this falsification of data could also be used, for example, in the context of fraudulent monitoring of food, industrial or energy supply chains.

Many crypto-currencies (Bitcoin, Ethereum Classic...) already suffered a 51% attack. Two things can prevent this kind of attack:

- having a **sufficiently decentralized hashrate** thanks to a balanced distribution of mining between several groups of miners
- Having a **sufficiently large number of nodes** so that the validation of the transmitted information can be invalidated in case of mining corruption.

STAKING



In the context of proof of stake, the tasks of miners have been divided into several roles, but the end goal nevertheless remains the same: Make sure that the information is transmitted correctly while respecting a peer-to-peer consensus, but this will be done with a completely different method.

Instead of solving mathematical equations with dedicated machines for this, it is the proof of possession of a certain amount of crypto that will allow a validator to validate transactions and put them in a new block. This way users no longer have to spend transaction fees and block rewards are distributed to different validators across the network.

The quantity of crypto to have beforehand is generally quite large (32 ETH for ETH2 for example) but this “participation” in the network is necessary to prove the seriousness of the candidates for validation.

There are several variants of Proof of Stake such as a mix between Proof of Work and Proof of Stake (Cardano) or Delegated Proof of Stake (EOS and WAX) but the concept remains the same. DPoS allows a user to stack his tokens in order to choose his trusted validator and in this way he receives a percentage of the block reward proportional to the frozen stake. This way the validator’s proof of stake is participatory and does not touch the full block reward.

Without being exhaustive, here are the advantages of PoS and DPoS:

- Greener for environment
- More transactions supported at the same time
- Faster transactions

And the disadvantages:

- Encourages nepotism
- Centralization of validation by whales

The balance of these consensus methods is found at the level of the number of crypto (or token) necessary to be a validator but also of those who are “contributors”, namely those who have decision-making power on the changes to be made at the consensus level.



6 **NFT &** HUMAN MINING



We will talk about the use of NFTs in Decentralized Finance (DeFi) in more detail in another chapter, it is about talking about a completely different view of things from mining as explained above.

NFT Mining



One way to mine that appeared in 2019 is to use NFTs as, so to speak, Proof of Collateral. Indeed, Chain Guardians, ahead of their time in many ways and the first, yielding passive income from deploying rare and popular NFTs to earn CGC the in game currency. By simply showing proof of membership of an NFT in your wallet, it is possible to have a chance of receiving an in-game block reward.

At the end of 2020, Rplanet uses roughly the same principle, but with a big difference. Like DoodleGod, the game consists of mixing items together to create new ones. The first items can be purchased with Aether which can be obtained by storing NFTs from partner projects with Rplanet.

While ChainGuardians only checks for proof that you actually hold NFTs, those staked in Rplanet are frozen in the project until they are unstaked.

Human Mining

By asking the user to actively participate in the project, he is rewarded in the form of NFT, tokens or even cryptos and this acts as time-stamped proof of his investment in the project. In this way, it is possible to publicly check whether the information coming from a user is reliable from his experience in the project.

The most telling example is that of blockchain games, which is sometimes referred to as "Proof of gameplay" since depending on the level of decentralization of the game, a greater or lesser number of actions will be recorded on the blockchain.

Some examples of video games using NFTs as the pivotal elements of this use:

Neon District where your team (each character is an NFT) allows you to collect NEON, the in-game currency of the game.

Alienworlds uses NFTs as the main element of the gameplay: all assets are in the game. Mining lands with your equipment not only gives you the fungible token in the game, but also a chance to find new pieces of equipment.

The challenge for the developers of these games is to find a balance between "pay to win" and a fair reward for the "early adopters" of the game so that everyone can have a chance to advance in the game without having to spend a fortune to catch up with the first arrivals.

Here again, we will come back to the concepts of Play to Earn, Blockchain and Crypto Gaming in more detail in other chapters.

Outside of video games, other industries have considered another way to use NFTs: that of certifying that a task has been completed, a skill acquired or a goal achieved.

Here are a few examples:

- It is possible to take courses on Gitcoin and once the final exercises have been passed and validated, the user obtains an NFT which acts as a certificate.
- Likewise, Binance distributes "diplomas" in the form of NFTs if the courses offered by the platform have been learned.
- There is also the [Microsoft Azure Certification](#) program which was designed in partnership with Enjin in 2019

Because of their form of standard on the blockchain, these certifications can be obtained in a secondary market and one would think that this facilitates fraud.

But since the only way to get them initially is to work hard, recruiters who want to verify the origin of the certificate will only have a quick glance at the blockchain!



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

We have published this series of guides in the purpose to educate people to understand the NFT market and give them the necessary knowledge to develop all tools necessary to navigate in 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