

# NFTs & Token Standards

A Standalone Mini-Course

BSc Blockchain Course

# Why Would Anyone Pay Millions for a JPEG They Cannot Touch?

In March 2021, a digital artwork sold at Christie's auction house for sixty-nine million dollars. The buyer received no physical canvas, no printed copy, no exclusive viewing rights. Anyone can still download the exact same image file from the internet for free. And yet the sale was real – the price was real – and the concept it validated now underpins a multi-billion-dollar market.

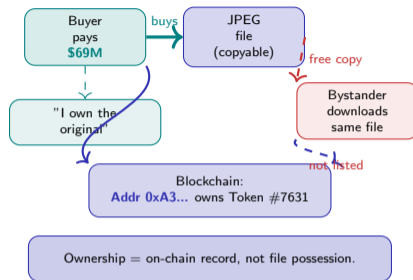
## The paradox this raises:

- What does it mean to “own” something digital if anyone can copy it?
- Can ownership exist without physical exclusivity?
- What exactly did the buyer of that JPEG receive?

The answer is not in the image file – it is in the blockchain record that says one specific address holds the authenticated original. Ownership became a verifiable fact on a public ledger, independent of who holds the file.

An NFT does not prevent copying – it records provenance. The value proposition is verifiable authenticity on a public ledger, not scarcity of bits.

**NFT = a blockchain record that proves one address holds the authenticated original of a digital item.**



## Think About Something You Own Digitally – Do You Really Own It?

You almost certainly own digital things: songs on a streaming platform, ebooks in a cloud library, in-game items you spent real money on, a playlist you spent hours building. But look at the terms of service. In almost every case, you do not own those items – you hold a revocable licence. The platform can withdraw it at any time.

### Quick Exercise – Think Before We Continue

- 1 **What happens if Spotify deletes your playlist, or Amazon closes your Kindle library?** You chose the music. You curated the list. Can you move it to another service? Can you sell your account? Can you leave it to someone in your will? Write down what you actually control.
- 2 **Have you ever bought an in-game item – a skin, a weapon, a character?** If the game shuts down tomorrow, what do you have? Could you sell it to another player on a different platform? What would it mean to “truly own” a game item the way you own a physical trading card?
- 3 **What would change if the asset lived on a public blockchain instead of inside a company’s database?** Think about portability, resale, persistence. What new risks would that introduce?

*Bring your examples to class. We will use them to test whether NFTs solve the problem – or just move it.*

---

**Digital licences are not ownership. NFTs are the first attempt to make digital ownership as persistent as physical possession.**

# What Makes a Token Non-Fungible?

## Token types compared across five dimensions:

Type	Standard	Unique?	Divisible?	Interchangeable?	Example use
Fungible token	ERC-20	No	Yes	Yes (1:1)	Currency, governance votes
Non-fungible	ERC-721	Yes	No	No	Art, deeds, credentials
Semi-fungible	ERC-1155	Configurable	Partial	Within class	Game items, event tickets
Soulbound token	EIP-5114	Yes	No	No (locked)	Diplomas, reputation

## The key distinction – fungibility:

Two ERC-20 tokens of the same type are perfectly interchangeable – like two ten-euro notes. One ERC-721 token has a unique `tokenId` that maps to a specific owner address in the contract. Swapping token #1 for token #2 is not the same exchange – one might represent a Rembrandt, the other a doodle.

Non-fungibility is a property enforced in code: each token has a unique identifier and a unique owner. The token standard defines the interface; the blockchain provides the permanent record.

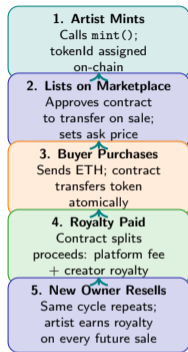
ERC-721: each `tokenId` is unique, each `ownerOf` maps to exactly one address – that is the technical definition of non-fungibility.

## What an NFT contract stores:

- **tokenId:** An integer, unique within the contract. Token #0, #1, #2 are distinct objects.
- **ownerOf(tokenId):** A mapping from token to address. The contract always knows who holds each token.
- **tokenURI(tokenId):** A URL or IPFS hash pointing to the metadata (name, description, image link, attributes).
- **transferFrom():** The function that moves a token from one address to another – on-chain, recorded permanently.

*The contract enforces the rules; the blockchain records the history. Neither can be overridden by the creator once deployed.*

# Follow One NFT from Minting to Resale – Every Step On-Chain



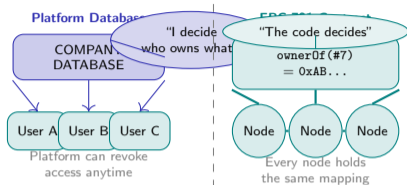
## Step by step – in plain language:

1. The artist calls `mint()` on the ERC-721 contract. A new tokenId is assigned. The artist's address is recorded as owner. The metadata URI points to the artwork. Gas fee paid; creation is permanent.
2. The artist lists the token on a marketplace (e.g. OpenSea). This grants the marketplace contract permission to transfer the token on a successful sale – a separate on-chain approval.
3. A buyer submits a transaction. The smart contract atomically transfers the token to the buyer and the ETH to the seller. No escrow, no intermediary.
4. The contract reads the royalty configuration (EIP-2981) and routes a percentage – say 5% – back to the original artist automatically.
5. Ownership now belongs to the buyer. They can hold, list, or transfer the token. On every future sale the royalty fires again – indefinitely.

The entire lifecycle – from creation to every subsequent resale – is recorded on-chain and enforced by code. The original artist earns automatically from secondary markets without any further action.

**Five steps: mint, list, purchase, royalty split, resale – all atomic, all permanent, no intermediary required.**

# How Does a Smart Contract Know This Token Is Yours?



## How ownership is verified without a central party:

- **Traditional platform:** Your "ownership" is a row in the company's database. The company can delete the row, restrict access, or go bankrupt. You have no independent proof.
- **ERC-721 contract:** The `ownerOf(tokenId)` mapping lives on a public blockchain replicated across thousands of nodes. No single party can change it – only a transaction signed by the current owner can transfer the token.

## Verification in practice:

- Any wallet can call `ownerOf(#7)` and receive the owner address
- Any marketplace can verify ownership before listing
- Any smart contract can check ownership as a condition (e.g. token-gated access)

*The proof is public, permanent, and requires no trust in any single institution.*

NFT ownership is not a belief – it is a verifiable state in a public contract. Any application anywhere in the world can read that state and act on it without asking anyone for permission.

**`ownerOf(tokenId)`: the single function call that proves ownership to any verifier, anywhere, without intermediaries.**

# The Floor Price Crashed Ninety Percent – What Went Wrong?

## NFT Market Boom and Collapse (2021–2022) At the peak of the NFT market

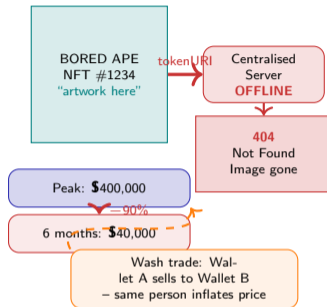
in early 2022, a Bored Ape Yacht Club NFT traded for over \$400,000. Six months later the same token traded below \$40,000. Some collections that had sold for tens of thousands of dollars became worthless within weeks.

### Three structural problems fuelled the crash:

- **Wash trading:** Sellers traded tokens between their own wallets to create artificial volume and price signals, deceiving buyers about genuine demand
- **Metadata fragility:** The NFT token is on-chain – but the image it points to often lives on a centralised server. That server can disappear, returning a 404 instead of your artwork
- **Speculation without utility:** Most buyers held no belief in the underlying value – only that a greater fool would pay more tomorrow

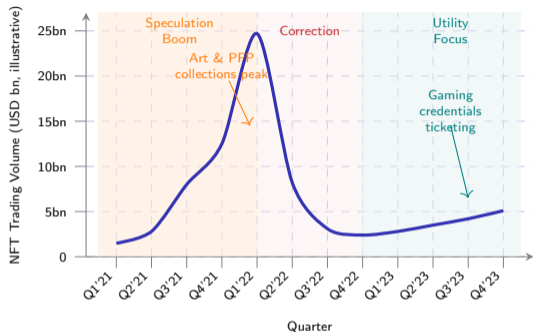
*The blockchain record of ownership survived. The value attached to it did not.*

The on-chain token is permanent – the value, the image it references, and the market around it are not. Owning an NFT when its metadata server goes offline means owning a pointer to nothing.



**NFT risk: token permanence does not protect against market collapse, wash trading, or off-chain metadata loss.**

# Beyond Bored Apes: Where Are NFTs Creating Real Value?



Illustrative

trend based on published market data. Not investment advice.

## Three phases – three different use cases:

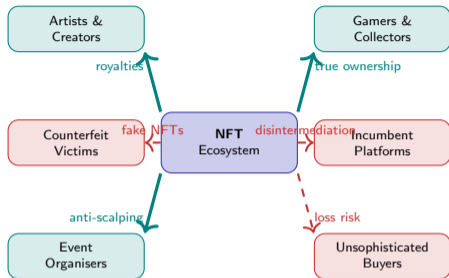
- **Speculation phase:** Profile-picture collections (Bored Apes, CryptoPunks) drove most of the volume. Buyers held tokens as status symbols and speculative assets. Most value was narrative, not utility.
- **Correction:** Interest rate rises, platform scandals, and wash-trading revelations deflated speculative premiums. Over 90% of NFT collections lost most of their value by mid-2022.
- **Utility focus:** Surviving projects shifted to genuine use cases – event ticketing (anti-scalping, automated royalties), gaming (cross-game item portability), verifiable credentials (diplomas, certifications), and real-world asset tokenisation.

*The hype inflated; the technology remained. The surviving use cases are those where programmable ownership solves a real problem.*

NFT trading volume collapsed because speculation ran ahead of utility. The projects that survived did so by solving a genuine problem: provable ownership of something people actually needed to own.

**Real NFT value = utility first: ticketing, credentials, gaming – not speculation on digital profile pictures.**

# Who Benefits from Programmable Ownership – And Who Gets Hurt?



## The same technology – very different outcomes:

**Artists:** For the first time, creators earn automatically from every secondary sale via smart-contract royalties. A musician who sold a track in 2021 earns a percentage every time it resells – indefinitely.

**Gamers:** In-game items that are NFTs can be sold peer-to-peer or used across multiple games. The player's investment survives even if the game shuts down.

**Event organisers:** NFT tickets cannot be counterfeited. Royalties on resale can be directed back to the venue, reducing scalper profits.

**Unsophisticated buyers:** No regulator, no recourse, no customer support. A wallet-draining scam or a project abandonment leaves buyers with worthless tokens and no one to call.

**Counterfeit victims:** Anyone can mint an NFT claiming to represent a famous artwork. The blockchain proves you own that specific token – not that the claim is legitimate.

Programmable ownership is neutral: it amplifies whatever intention is behind the transaction – artist empowerment or sophisticated fraud. The technology does not distinguish.

**NFTs redistribute value toward creators and away from platforms – but also create new attack surfaces for fraud and speculation.**

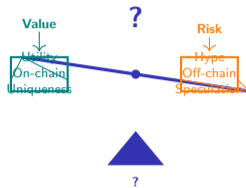
# Three Tests for Lasting NFT Value

Before accepting any NFT use case as genuinely valuable, ask:

- T1 Does this use case require provable, transferable uniqueness?** If the value comes from uniqueness that must be publicly verifiable and transferable between parties who do not trust each other, NFTs earn their cost. If a centralised database with access controls would do the same job, it almost certainly should.
- T2 Does the metadata and the value live on-chain – or on a server that might disappear?** An NFT pointing to an image on a centralised server is only as permanent as that server. Genuine durability requires on-chain metadata or a decentralised storage protocol (IPFS, Arweave). Ask: what happens if the project team disappears tomorrow?
- T3 Is there underlying utility beyond the expectation that someone will pay more later?** Event access, royalty revenue, game interoperability, and verifiable credentials all provide value independent of price appreciation. Pure speculative collections fail this test. If the only use case is resale, you are the last buyer.

An NFT is not valuable because it is an NFT. It is valuable when programmable ownership solves a real coordination problem that no simpler tool could solve as well.

Apply T1–T3 to every NFT proposal: provable uniqueness needed? On-chain metadata? Utility beyond resale?



T1–T3 tell you which side weighs more.  
All three pass = genuine value candidate.

Quick

diagnostic:

- All three YES → strong candidate for lasting value
- Two YES, one NO → evaluate the missing dimension carefully
- One YES or fewer → high probability of speculative collapse

## Your Challenge

Read the case below, then apply the three tests from the previous slide.

### Case: University Diplomas as NFTs

**Situation:** A university wants to issue degree certificates as NFTs on a public blockchain so that graduates can prove their credentials to any employer worldwide without contacting the registrar. The university would mint one NFT per graduate at the time of graduation. The token would contain the graduate's name, degree, date, and a cryptographic hash of the official transcript. Employers could verify the credential by reading the on-chain record directly.

Apply the three tests. Fill in the table below:

Test	Your answer (Yes / No / Partial)	Reasoning (one sentence)
T1: Provable transferable uniqueness required?	.....	.....
T2: Metadata and value durable on-chain?	.....	.....
T3: Utility beyond resale expectation?	.....	.....

**Discuss with your neighbour (3 minutes):** Is this a genuinely good NFT use case – or could a signed PDF and a public verification API do the same job? What additional design decisions (transferability, metadata storage, who controls minting) would determine whether this succeeds or fails? Where do you disagree?

The best NFT use cases solve a real verification problem. Ask whether the blockchain adds something a database and a signature cannot.