The Illusion of Ownership in Digital Art

Why a “Sale” of a Digital Asset Cannot Transfer True Ownership or Control to the Consumer

A Technical and Legal Position Paper for Regulators and Legal Practitioners

Author	Amir Soleymani

Document type	Consumer-protection position paper / technical-legal analysis
Date	20 June 2026
Intended readership	Digital asset regulators, consumer-protection authorities, courts, and legal practitioners across all jurisdictions
AI Disclosure	AI-assisted drafting tools were used in the preparation of this paper. All analytical positions, factual verification, legal arguments, technical findings, and conclusions are the author's own.

Status: *This paper advances an analytical position. The technical findings on which it relies are drawn from publicly verifiable sources — blockchain records, HTTP responses, DNS records, smart-contract source code, and public platform notices — and are independently reproducible by any third party. Where the paper draws legal inferences, those inferences are identified as argument, not as settled law.*

Author: Amir Soleymani

Document type: Consumer-protection position paper / technical-legal analysis

Date: 20 June 2026

Intended readership: Digital asset regulators, consumer-protection authorities, courts, and legal practitioners across all jurisdictions

AI Disclosure: AI-assisted drafting tools were used in the preparation of this paper. All analytical positions, factual verification, legal arguments, technical findings, and conclusions are the author's own.

Status: This paper advances an analytical position. The technical findings on which it relies are drawn from publicly verifiable sources — blockchain records, HTTP responses, DNS records, smart-contract source code, and public platform notices — and are independently reproducible by any third party. Where the paper draws legal inferences, those inferences are identified as argument, not as settled law.

Table of Contents

1. Executive Summary

The harm, in brief

Since 2017, consumers around the world have spent tens of billions of dollars purchasing digital artworks sold as non-fungible tokens ("NFTs") on the promise of permanent, immutable ownership. At least seven major NFT platforms have shut down or permanently closed between 2017 and 2026. An estimated 650,000 NFTs hosted on a single platform — Nifty Gateway — were placed at risk when that platform announced closure in April 2026. MakersPlace, the platform that minted the NFT for the Christie's sale of Beeple's *Everydays* at US$69.3 million, announced closure on 16 January 2025. Foundation, which processed over US$230 million in primary sales, closed permanently in April 2026 after an acquisition by Blackdove collapsed. In every case, the tokens survived on the blockchain. In most cases, the art did not.

This is not a story about bad actors. It is a story about a structural mismatch between what consumers are told they are buying and what the technology actually delivers.

The central finding

A "sale" of a digital artwork — in the ordinary and legal sense of transferring ownership and control to the buyer — does not, on prevailing market practice, occur. A collector sees an artwork, is drawn to it, and pays for a token marketed as securing blockchain-guaranteed ownership of that artwork — permanent, immutable, verifiably theirs. What they receive is a token that genuinely has those properties, attached to an artwork that has none of them. The blockchain's properties — immutability, verified scarcity, transparent provenance — apply to the token record. They do not, and cannot, apply to the image or video stored on someone else's server, controlled by someone else's contract, accessible only through someone else's infrastructure. The structural dependency is inherent to the transaction design.

Four independent structural failures make true ownership impossible:

1. **The smart contract is controlled.** The artist or platform can change what the token points to — altering, redirecting, or destroying the artwork — at any time, without the holder's consent and often without any trace.

2. **The asset is not stored with the owner.** The artwork lives on private corporate servers, or at best on decentralised storage dependent on third parties continuing to pay for it. Either can disappear, leaving the token pointing to a blank page.

3. **Access to the blockchain is centralised.** In practice, nearly all consumers reach the blockchain through a handful of commercial gateway providers who have already restricted access from certain jurisdictions and can do so again.

4. **The asset cannot exist without infrastructure.** A digital artwork requires electricity, a device, software, and usually the internet just to be seen. Remove any of these and the artwork does not exist — a constraint that does not apply to a physical painting.

The regulatory gap

An NFT is sold as an outright purchase but functions as a subscription service: the buyer pays in full, up front, for access that depends entirely on a provider's continued operation and good faith. Streaming services and software subscriptions, which are honest about precisely this dependency, are regulated accordingly. NFTs — which carry the same dependency while marketing the opposite — are not. The consumer in the least-protected, worst-disclosed position is also the one who paid the most, for the longest commitment.

What this paper asks of regulators and practitioners

This paper does not call for a ban on digital art or blockchain technology. It calls for three things that should be uncontroversial in any developed legal system:

- **Honest marketing:** prohibit the unqualified use of "own," "permanent," and "sale" where the facts do not support those terms.
- **A standardised point-of-sale disclosure label** that tells buyers, in plain language, where the artwork is stored, who controls it, and what happens if the platform closes.
- **Classification of dependency-bearing NFTs as service transactions** for consumer-protection purposes, attracting the same disclosure and continuity obligations that apply to subscription services.

The analysis, the evidence, and the recommendations that follow apply regardless of jurisdiction. The structural failures described are built into the technology; the regulatory gap exists wherever NFTs are sold.

---

2. Purpose, Scope, and Method

2.1 Purpose

This paper assists regulators, consumer-protection authorities, courts, and legal practitioners in understanding a structural consumer-protection problem in the digital-art market, and proposes

practical measures to address it. It is not directed at any single jurisdiction: the technical failures described exist wherever NFTs are sold, and the recommended responses reflect principles — disclosure, honest marketing, service-appropriate regulation — that are common to every developed consumer-protection regime.

2.2 Scope

The paper concerns **art and collectible NFTs sold to consumers** — tokens whose value lies in an associated image, video, or other media file. It does not address fungible cryptocurrencies or copyright as such. Copyright is mentioned only where it bears on the gap between what a consumer believes they are buying and what they actually receive.

One category warrants explicit acknowledgement rather than exclusion: generative works that store their core data directly in the smart contract's bytecode. These projects occupy a spectrum, and clinical precision is required.

At one end sits a small number of projects — Autoglyphs being the clearest example — that store both the generative parameters and the complete rendering logic entirely within the contract itself. The contract outputs the artwork directly from on-chain computation, with no dependency on any external file, server, or code library. These works genuinely survive all four structural failures described in Section 5: the contract cannot point to a dead URL because there is no URL; the media cannot disappear from a server because it is not on a server; the artwork exists for as long as the blockchain exists and the Ethereum Virtual Machine can execute the contract's code. In this configuration, the technology does deliver what the market as a whole claims to sell.

Most generative NFT projects — including the majority of Art Blocks collections — do not meet this standard. A typical Art Blocks collection stores a generative JavaScript script on-chain, which is genuine and meaningful. However, that script typically depends on an external rendering library — most commonly p5.js — served from a CDN endpoint or external web framework to execute in a browser canvas environment. If that CDN endpoint changes its API specification or goes offline, the on-chain script executes but outputs an empty or broken canvas. The artwork fails to render not because the on-chain data is gone, but because the execution environment it depends on is no longer accessible. This is a residual Failure Two dependency at the rendering layer rather than the storage layer. The distinction matters: storing generative parameters on-chain is materially better than hosting a static image on a private server, but it is not equivalent to a fully self-contained on-chain system unless the complete execution environment is also on-chain or natively supported by the underlying node software.

The technically correct formulation is: only projects storing both the generative parameters and the complete rendering engine entirely on-chain — or relying exclusively on execution environments natively implemented in the core blockchain node software — fully survive Failure Two. Projects that store parameters on-chain but depend on off-chain JavaScript libraries for rendering retain an operational dependency at the execution layer. This paper's argument applies to the more than ninety-nine percent of the market operating with off-chain storage or off-chain rendering dependencies. The existence of genuinely self-contained on-chain configurations, however rare,

demonstrates that genuine digital ownership is technically achievable and that the industry's failure to adopt the standard is a matter of choice rather than technical necessity.

2.3 Method and evidentiary standard

Every technical assertion is of a kind that can be independently reproduced by any third party using public tools: on-chain data (token ownership, transfer history, contract owner, contract source code) read directly from the blockchain; infrastructure data (hosting location, file-modification dates, operators) read from public HTTP headers and DNS records; and platform statements quoted from public notices. Where a figure or date is given, it can be checked. Where the paper reasons from fact to a legal or commercial conclusion, that reasoning is presented openly as argument, not as settled law.

Where code examples and specific case studies reference EVM-specific standards — including ERC-721, EIP-2981, and Solidity contract patterns — they do so for illustrative consistency; the structural mismatch between an immutable on-chain token record and mutable or dependency-bearing off-chain media is a mathematical reality common to all token architectures, regardless of whether the underlying protocol is Ethereum Layer-1, an EVM-compatible Layer-2 (such as Base, Arbitrum, or Optimism), Solana, Bitcoin Ordinals, or any other blockchain or scaling layer. The specific standard names and bytecode patterns differ across chains; the structural gap they illustrate does not.

---

3. What an NFT Is, What It Promises, and What It Delivers

3.1 Plain language first: what NFTs are and why people buy them

Before examining what the law says and what the technology does, it is worth establishing — in plain language — what an NFT is, what problem it was invented to solve, and what a collector actually experiences when they make a purchase. This foundation matters because the legal and technical arguments that follow only make sense against the backdrop of what the consumer believed they were getting.

3.1.1 The problem NFTs were designed to solve

Before NFTs existed, digital art faced a fundamental commercial problem: infinite copyability. A digital image — a JPEG, a video, a piece of generative art — can be copied perfectly and at zero cost by anyone with a computer. Every copy is identical to every other copy. There is no original. This made digital art commercially worthless as a collectible in the traditional sense, because scarcity — the condition that gives a physical painting or a limited-edition print its value — simply did not exist in the digital realm.

NFTs were adapted and marketed as the technical solution to this problem. The idea was straightforward: even if the image itself could be freely copied, the blockchain could create a verifiable, unforgeable record of who owns the "official" token associated with that image. Scarcity

would be manufactured not in the image but in the token. The token would be the scarce, ownable thing; the image would be what the token represented.

3.1.2 What a blockchain is

A blockchain is a shared record book maintained simultaneously by thousands of computers around the world, designed so that no single party controls it and no entry, once recorded, can be altered or deleted. Every transaction is permanently and publicly visible. The design is deliberately resistant to central control: there is no company that owns it, no server that hosts it, no administrator who can edit it. This is what is meant when blockchain technology is described as "decentralised" and "immutable" — the ledger itself cannot be rewritten.

These are genuine properties of the underlying technology. They are also the properties that were sold to consumers as applying to the digital artworks they were buying. As this paper establishes, they do not.

3.1.3 What an NFT actually is

An NFT — a non-fungible token — is a unique entry in a blockchain's record book. "Non-fungible" means it is not interchangeable with any other token: unlike a unit of currency where one pound is identical to any other pound, each NFT is distinct. The entry records three things: a token identifier, the wallet address that owns it, and a location — a web address — where information about the token can supposedly be found.

That web address points to a metadata file — a small text document containing a title, description, and link to the actual image or video. The image or video is stored separately, typically on a company's web server.

This is the structure in full: blockchain record → web address → metadata file → image link → image. The blockchain secures only the first step. Every subsequent step depends on infrastructure, companies, and decisions that the buyer does not control.

3.1.4 Why the collector's motivation is central to the legal analysis

A collector does not look at a token identifier and decide to buy it. They look at an artwork. They see an image, a video, a piece of generative art. They are drawn to it — for aesthetic reasons, for cultural reasons, because the artist matters to them, because they believe it will hold or increase in value, because owning it carries status in a community they belong to. Whatever the reason, the decision to purchase is a decision about the *artwork*. The token is the mechanism of purchase, not the object of desire.

This is the moment at which the misrepresentation begins. The collector sees the artwork, decides they want to own it, and is presented with a purchase that implicitly or explicitly promises them blockchain-guaranteed ownership of that artwork — permanent, immutable, verifiably theirs. They pay, often a very large sum. What they receive is a blockchain-guaranteed token, and access to an artwork that the blockchain does not touch.

The collector paid for the blockchain's properties to be applied to the asset. The blockchain's properties apply only to the token. The asset — the image, the video, the work they saw and wanted — receives none of them.

3.2 The blockchain properties that were sold as promises

The NFT market sold collectors on a specific set of properties that blockchain technology genuinely possesses. Understanding what those properties are — and recognising that they apply to the token, not to the artwork — is the foundation of the analysis that follows.

The properties that were sold:

- **Immutability.** Once recorded on the blockchain, the token record cannot be altered or deleted. The history of who owned what, and when, is permanent.
- **Verifiable scarcity.** The total supply of tokens in a collection is fixed at minting and cannot be inflated. A collection of 100 tokens cannot secretly become 200. It is important to be precise about what is scarce here: the *tokens* are scarce. The underlying image or video file is not — it can be freely copied and downloaded by anyone. The scarcity that collectors understood themselves to be purchasing — an authenticated, unique instance of the artwork — is exactly what the token cannot, on its own, deliver.
- **Decentralised ownership.** No single company controls the ledger. The buyer's token record does not depend on any platform staying in business (in the sense that the ledger entry itself is decentralised, though as Section 5.3 establishes, practical access to that ledger is not).
- **Transparent provenance.** Every transfer of a token is publicly recorded. The full history of a work — from minting to current holder — is visible to anyone.

These properties are real. The blockchain does deliver them. The problem is that they apply to the token — the row in the ledger — and not to the artwork the token represents. The artwork is stored elsewhere, controlled by others, and subject to none of these guarantees. What was sold as a package of properties securing the artwork is, technically, a package of properties securing a pointer to a web address where the artwork used to be.

This gap — between what the properties were sold as covering and what they actually cover — is the root misrepresentation from which every specific failure in this paper flows.

3.3 What "ownership" and "sale" mean in law

In every developed legal system, ownership of property connotes a bundle of rights that, at minimum, includes the right to possess the thing, the right to use and enjoy it, the right to exclude others, and the right to dispose of it. A "sale" is the transaction by which that bundle passes from seller to buyer for a price. The defining feature of a completed sale is that, afterwards, the thing is within the buyer's control and the seller can no longer unilaterally take it back, alter it, or destroy it.

A consumer told they are "buying" and will "own" a digital artwork reasonably understands these ordinary meanings to apply. The marketing language of the NFT industry — "own," "collect," "sale," "your asset" — is the language of property and transfer. Against the plain-language understanding

established in Section 3.1, the consumer's interpretation is not only reasonable — it is the interpretation any ordinary person would form when confronted with that language in that context.

A sophisticated legal respondent may argue that this classical framework is inapplicable to digital assets, and that the analysis above is tethered to an obsolete conception of tangible property. This objection deserves direct engagement. Common law jurisdictions are evolving their treatment of digital assets, and courts and law commissions in several jurisdictions — most notably the UK Law Commission in its 2023 report on digital assets — have proposed treating crypto-tokens and digital objects as a third category of personal property, distinct from both choses in possession (physical objects) and choses in action (enforceable legal rights). Under this framework, a platform or artist may also argue that the transaction constitutes a contract of bailment or a service level agreement, in which physical custody was never the legislative target and the "failure" of the server is simply an operational risk or breach of contract rather than a non-sale.

The paper does not dispute that digital assets may warrant a distinct legal category. The argument survives intact even on the most generous reading of the emerging intangibles framework. The core rights of any ownership category — whether framed in classical property terms or under a novel intangibles classification — include at minimum the right to exclude others from the asset and the right to extract utility from it. Both rights are structurally broken in the typical NFT transaction. The holder cannot exclude others: the artist retains the technical power to redirect the pointer; the platform retains the power to modify or delete the hosted file; and, as Section 6.5 establishes, any third party can hold an identical copy of the underlying file with no less claim to it than the "owner." The holder cannot reliably extract utility: the file may disappear when the platform closes, the token may point to nothing, and access depends on infrastructure the holder does not control. The argument is therefore not that digital assets must be treated as physical property to trigger consumer protection. It is that whatever category a court or regulator assigns to an NFT, the rights associated with that category are not delivered.

3.4 What an NFT actually is, at the technical level

An NFT is not the artwork. Technically, an ERC-721 token (the dominant standard on Ethereum) is a record in a smart contract associating a token identifier with an account address, together with a function, `tokenURI`, that returns a *location* where the token's metadata can supposedly be found. The metadata is a separate file that, in turn, contains a link to the image or video.

Critically, the ERC-721 standard **does not require** that the `tokenURI` point to decentralised or permanent storage, **does not require** that the content at that location be immutable, and **does not require** any cryptographic binding between the token and the artwork. The standard provides only that the function returns "a distinct Uniform Resource Identifier (URI) for a given asset." That URI may point anywhere, and — as Section 5 shows — it can usually be changed at will.

There is a further constraint that the standard does not impose, and that the blockchain cannot enforce: **it does not verify that the person minting a token has any right to do so, or that the name, identity, or wallet address stated in the metadata belongs to the person it claims to represent.** The implications of this are significant and are addressed in Section 3.7 below.

3.5 The token is not the asset — and an art NFT is not a currency

A crucial distinction is routinely blurred in public debate: an art NFT is **not** the same kind of thing as a fungible cryptocurrency such as ETH or Bitcoin, and treating it as one obscures the harm.

With a fungible cryptocurrency, the token *is* the asset. A unit of Bitcoin has no separate "underlying" object; its value, whatever one thinks of it, is intrinsic to the token itself, and the immutable ledger genuinely secures the entire thing of value. Ownership of the token is ownership of the asset, completely.

With an art NFT, this is not so. The collector did not decide to buy a token. They decided to buy an artwork. The token is the instrument by which that purchase was effected — but the artwork, and the blockchain properties the buyer believed would protect it, are two different things pointing in opposite directions. The blockchain properties protect the token. The artwork is protected by nothing the blockchain controls.

3.6 The gap

The result is a fundamental gap between what the consumer believes they bought (an artwork they now own and control, secured by blockchain properties) and what they actually received (a token secured by blockchain properties, associated with a changeable pointer to a file held by others, viewable only through technology they do not control). The token is genuinely theirs and genuinely immutable. The *art* — the thing they saw, wanted, and paid for — is none of those things.

One further dimension of the gap is worth stating plainly, though a full treatment of copyright is outside the scope of this paper: in the absence of an explicit written agreement to the contrary, the purchase of an NFT does not transfer copyright in the underlying work. The buyer acquires the token. The artist retains the copyright. A consumer who paid a significant sum believing they "own" the artwork has, in most jurisdictions, acquired neither control of the artwork nor any of the rights that copyright confers — including the right to reproduce it, display it commercially, or prevent others from doing so. This compounds the misrepresentation: what was sold as full ownership of a digital artwork is, in practice, a revocable database entry associated with a file the buyer cannot legally control, commercially exploit, or permanently access.

Everything that follows is an elaboration of that gap and of why the buyer's own diligence cannot, on current market practice, close it.

3.7 Two further failures the provenance claim cannot survive

Independent of the structural failures examined later in this paper, the proposition that an NFT token constitutes a reliable provenance record faces two additional problems that are independent of platform conduct or storage architecture. Both go to the integrity of the chain of ownership itself.

3.7.1 The blockchain does not verify who is minting

When an NFT is minted, a wallet deploys a smart contract (or mints through an existing shared one) to the blockchain. The blockchain records the deploying wallet's address faithfully and permanently — this is the address that appears on block explorers and marketplace interfaces as the "creator" of the collection. What the blockchain cannot do, and does not attempt to do, is verify that the person controlling that wallet is who they claim to be, or that they had any right to mint what they minted.

To understand why this matters, it is necessary to understand what a wallet address actually is. A wallet address is a pseudonymous identifier — a string of characters derived mathematically from a private key. It has no inherent connection to any real-world identity. The address `0xABC...` tells you nothing about who controls it. The blockchain records that a transaction was signed by the key corresponding to that address. It cannot record, and has no mechanism to verify, whether the person signing is Beeple, a gallery representing Beeple, or a complete stranger who has no connection to Beeple whatsoever.

The metadata of an NFT — the file that contains the artwork title, artist name, description, and image link — is written by the minter and submitted as part of the deployment. It can say anything. A person wishing to impersonate a well-known artist needs only to: deploy a standard ERC-721 contract from any wallet they control; write metadata that states the artist's name, references their known works, and links to images copied from the artist's public portfolio; mint tokens from that contract; and list them for sale on a marketplace. The resulting blockchain record shows a real transaction, a real contract address, a real creation timestamp, and whatever the minter chose to write in the metadata. Nothing in the protocol indicates whether the deploying wallet has any connection to the named artist.

A consumer examining this on a marketplace faces a practical impossibility. They see a wallet address listed as "creator." To determine whether it is genuine, they would need to independently know the artist's verified wallet address — information that is not consistently published, not displayed on most marketplace interfaces in a form consumers can act on, and not something that can be checked without already knowing the answer. The marketplace may display the wallet address; it cannot tell the consumer whether that address belongs to the claimed artist. That determination requires off-chain knowledge the consumer does not have.

This is not a theoretical risk. In one documented period, OpenSea reported that approximately 80 percent of NFTs minted using its free minting tool — a tool with no cost barrier and therefore attractive to high-volume fraudsters — were counterfeit, plagiarised from other artists, or spam. Artists across the market have discovered collections in their names, minted from wallets they do not control, containing images taken from their public portfolios without consent. The blockchain recorded all of these transactions as accurately as it recorded any genuine mint. It had no mechanism to distinguish them.

The significance for the provenance claim is direct and serious. If the blockchain record of "creator address" does not establish that the creator was the named artist — because the address is pseudonymous, because no identity verification occurs at the protocol level, and because a consumer cannot independently verify the connection without off-chain knowledge — then the chain of provenance the token is supposed to represent begins on an unverifiable foundation. The

blockchain recorded who signed the transaction. It did not record whether that person had any right to create what they created, or any connection to the art they named.

3.7.2 Wallet loss severs the ownership chain permanently

With a physical artwork, ownership and access are separable. If a collector loses the key to their storage facility, the painting still exists, and ownership can be established through purchase receipts, insurance records, auction house documentation, gallery records, correspondence, photographs, and witness testimony. The law has centuries of developed practice for establishing title through paper trails. Losing physical access to a property does not extinguish legal title to it.

With an NFT, the wallet is not merely the means of access — it is the proof of ownership. There is no secondary record, no registry, no parallel paper trail. The only mechanism by which a holder can prove they control a token is by signing a cryptographic message with the private key of the wallet that holds it. Without that key, the proof cannot be produced.

Private keys are controlled through a seed phrase — a sequence of twelve or twenty-four words generated when the wallet is created. If that seed phrase is lost — through a forgotten backup, a dead device, a house fire, the death of the holder, or theft — the private key is gone permanently. No legitimate service can recover it. The mathematics of elliptic curve cryptography, on which all major blockchain wallets rely, make recovery without the seed phrase computationally impossible with current technology. The blockchain will continue to show the token sitting in the wallet address; the holder simply has no way to prove they control it or to move it.

The consequences extend beyond the holder themselves. If the minting artist loses access to their original wallet — the wallet whose address is on-chain as the creator — they can no longer cryptographically prove they are the creator of the work. Someone else who downloads the artwork and claims to have lost their "purchase" wallet can now make an equivalent claim. The provenance chain that was supposed to run from artist to collector through immutable blockchain records is dependent at every link on every party in that chain having retained access to their seed phrase — a credential that no institution maintains, no court can compel production of, and no authority can restore.

The provenance claim requires not just that the blockchain record is accurate, but that both artist and collector — and every intermediate owner — have retained uninterrupted access to the wallets that participated in the chain. Break any link, and the chain of proof is gone. This is not analogous to losing a key to a storage facility. It is analogous to a legal system in which title to property can only be proved by producing a cryptographic credential that exists nowhere except in the owner's private keeping, with no institutional backup, no court remedy, and no recovery if lost.

---

4. A Concrete Case: What Ownership Actually Looks Like in Practice

Before examining the structural failures in the abstract, it is useful to see them operating on a real, named collection. The following observations are drawn from publicly accessible sources — the

Ethereum blockchain, Etherscan's verified contract records, and Nifty Gateway's own public announcements — and are independently reproducible by any third party using the tools described in Section 13. They are offered as illustration of how the failures manifest in practice. The analysis in Section 5 stands independently of this example.

The collection in question is the **Beeple Spring Collection**, an ERC-721 contract deployed at address `0xdd012153e008346591153fFf28B0DD6724f0C256` on Ethereum, containing 511 tokens including the edition *ABUNDANCE*, associated with a US$650,000 auction sale conducted through the Nifty Gateway platform in April 2021. Contract state and metadata were verified via Etherscan and public RPC endpoints in March 2026 and confirmed current as of 20 June 2026; on-chain state is permanent and the observations below remain independently reproducible.

This example is not marginal. Beeple — the artist Mike Winkelmann — is among the best-known figures in the NFT art market, whose work at Christie's set a world record for digital art at auction. Nifty Gateway was, for a period, the dominant marketplace for high-value digital art drops, conducting sales across dozens of collections and hundreds of thousands of individual tokens. The Spring Collection alone comprised 511 tokens sold at individually significant prices; the total primary sales revenue has never been publicly disclosed by the platform. What the blockchain shows about this collection therefore describes not an obscure or experimental project but a mainstream, commercially substantial release — and one in which the structural conditions described below are the same conditions that applied across every sale Nifty Gateway ever conducted. The failures were not specific to this collection. They were the platform's standard operating architecture.

What the blockchain shows about contract control. The contract's verified source code, readable on Etherscan, contains a `setBaseURI` function restricted to the contract owner via the `onlyOwner` modifier. The deploying wallet — publicly tagged as Beeple — remains the contract owner. Ownership has never been transferred and has not been renounced: the owner address is not the zero address. This means the artist retains the unilateral power to redirect every token in the collection — all 511 of them — to any location, or to nothing, at any time, without notice to or consent from any holder. This is Failure One in operation on a live, high-value collection.

What the blockchain shows about storage and integrity. Calling `tokenURI` on any token in this collection returns a URL resolving to `api.niftygateway.com` — a company-controlled endpoint, not a decentralised or content-addressed location. The media associated with each token is served from commercial hosting infrastructure behind a CDN, not from IPFS or any on-chain source. The metadata for these tokens contains an `image_hash` field set to the literal string `"none"`. There is therefore no cryptographic binding between the token and any specific version of the media file. As Section 6.5 explains, the absence of an integrity hash means the token cannot function as a provenance record for any particular file: it certifies only that a URL once existed, not that the content at that URL is or remains the work originally sold. This is Failure Two in its most common form — and the same absence of integrity binding applied to the platform's entire catalogue.

What Nifty Gateway's public announcements show about custody and continuity. Nifty Gateway operated a custodial model in which tokens were held in the platform's own wallet and users held internal database entries rather than on-chain positions. The platform publicly announced

closure in April 2026, entering a withdrawal-only mode. Its commitment to host legacy metadata "in perpetuity" is a voluntary corporate undertaking — stated on a website belonging to a business in wind-down — not a technical guarantee, a contractual obligation enforceable by holders, or a commitment backed by decentralised storage. Every holder of every token ever sold through Nifty Gateway faces the same dependency on that undertaking.

Taken together, these publicly observable facts describe not just the condition of one collection but the structural reality of an entire platform's output. None of this required examining any individual account, any specific holder's position, or any disputed facts. It is visible to anyone with a block explorer and a browser. The following section explains why this condition is not particular to Nifty Gateway but is the predictable consequence of how NFT contracts and platforms are built.

---

5. The Four Structural Failures of Digital Art Ownership

The four failures are ordered from the most contingent (depends on someone's conduct) to the most fundamental (applies even when everyone behaves perfectly). Together they show that the gap identified in Section 3.6 is not an accident of a particular platform but is built into the architecture of digital art as it is currently sold.

5.1 Failure One — The Smart Contract Is Controlled by Others

5.1.1 The mechanism

Most NFT contracts build each token's metadata location by combining a stored "base URI" with the token's identifier. The base URI sits in a variable that the contract's owner can change through a function commonly named `setBaseURI`. In the widely used OpenZeppelin pattern it is as simple as:

```
function setBaseURI(string memory _newBaseURI) public onlyOwner {
    _baseTokenURI = _newBaseURI;
}
```

One function call, one transaction, and every token in the collection is simultaneously redirected to a new location. The `onlyOwner` restriction means only the contract owner can do this — but the contract owner is, in practice, the artist or the platform, **not the buyer**. The buyer has no equivalent power and no veto.

5.1.2 Why this defeats ownership

If the artist or platform can change where the token points — and therefore the name, description, image, and video the world sees — then the holder does not control the asset. They control only the token record; the substance remains in the gift of a third party. Two features make this worse:

- **No notice and no consent.** Such contracts require neither notice to, nor consent from, holders before the pointer is changed.

• **No reliable trace.** Many such contracts emit no event when the base URI changes, and in any event the *content at a fixed URL* can be changed at the server level without any contract transaction at all. The holder may have no way to know that the asset they "own" has been altered.

5.1.3 Two controllers, each fatal

There are usually **two** parties with power over the asset, and either alone destroys the buyer's control:

1. **The contract owner** (artist or deployer) can redirect the on-chain pointer.
2. **The server operator** (the platform hosting the metadata and media) can change the content served at the existing pointer, with no contract transaction at all.

A buyer who somehow trusted the artist would still be exposed to the platform, and vice versa. They must rely on the continued good faith, continued solvency, and continued operation of every such party, indefinitely. The only configuration that removes Failure One is **irrevocable renunciation of contract ownership** — transferring it to an address no one controls — after which the pointer can never be changed again. A minority of well-engineered collections do this; most do not.

5.2 Failure Two — The Asset Itself Is Not Stored With the Owner

5.2.1 The asset is off-chain

The image or video — the thing the consumer actually wanted — is, for the great majority of art NFTs, not stored on the blockchain. It lives off-chain, in one of two ways:

• **On private corporate servers** (a company's own API plus a commercial media host behind a cloud CDN). This is the most common and most fragile arrangement.

• **On decentralised storage (IPFS or Arweave).** This is materially better, but, in the case of IPFS, carries its own dependency described below.

5.2.2 The fragility of private servers

When metadata and media sit on a company's servers, the artwork's continued existence depends on a chain of commercial arrangements entirely outside the buyer's control: the company continuing to operate; the company continuing to pay its hosting and media bills; the domain name continuing to be renewed; and the relevant cloud accounts staying in good standing. A break at any single link renders the artwork inaccessible — while the blockchain still faithfully records that the buyer "owns" the token. The token now points to a "not found" page. As Section 8 documents, this has happened repeatedly across the industry.

5.2.3 The hidden dependency of IPFS — pinning and garbage collection

IPFS is frequently offered as the cure. It is a genuine improvement: because files are addressed by a hash of their content, the content cannot be silently swapped — change the file and its address changes, so a token pointing to the old address simply fails rather than showing altered content. But

IPFS does not by itself guarantee *permanence*. A file persists on IPFS only for as long as at least one node continues to **pin** it (store and serve it). Pinning is a service someone must pay for and maintain. If the artist, the platform, or their pinning service stops pinning — through cost-cutting, shutdown, or neglect — and no other node happens to hold the file, the content becomes unreachable even though the pointer is "decentralised." The buyer who relies on someone else's pinning again controls nothing.

The mechanism by which this occurs is IPFS garbage collection. IPFS nodes periodically run automated storage recycling protocols that evict unpinned content from their local caches to reclaim disk space. This is a routine, designed behaviour of the protocol, not a failure. When it runs, a file with no active pinner is deleted from that node's storage. If all nodes that held a copy have run garbage collection without replacement, the file ceases to exist anywhere on the network. Critically, the on-chain content address — the `ipfs://` URI recorded in the token's metadata — remains structurally valid. It points to a content hash that no longer resolves to any data. From the consumer's perspective, the outcome is identical to a 404 error on a private server: the token points to nothing, the artwork is gone, and the blockchain has no record of its disappearance. The difference in mechanism provides no practical difference in outcome.

This means the distinction between IPFS content-addressing and private server hosting is real but conditional. IPFS is materially safer only when active, verifiable pinning exists. A content address backed by a funded, programmatically verifiable storage contract — such as a Filecoin storage deal, which records the storage commitment on-chain, or Arweave's permanent storage model, which requires a one-time endowment that algorithmically funds perpetual storage — provides a meaningfully stronger guarantee than either passive IPFS propagation or private servers. Passive IPFS distribution, with no active pinner and no on-chain storage commitment, is vulnerable to garbage collection over time horizons well within the expected lifespan of a valuable artwork.

A further dependency exists even where the content genuinely is on IPFS: metadata often links through **a specific company's IPFS gateway URL** rather than the native, location-independent content address. When that company shuts down, the gateway URL breaks — even though the same content may remain retrievable through the decentralised network for anyone holding the underlying address. Applications that depend on the company gateway then display nothing.

5.2.4 The absence of integrity binding

A protection that would at least let a buyer *detect* tampering is a cryptographic hash of the media file, recorded in the metadata or on-chain. Where present and populated, it lets anyone verify that the file they are shown is the file originally sold. Where it is set to a placeholder such as the literal string `"none"`, there is no verification mechanism at all: content can be replaced and the buyer cannot prove it.

5.3 Failure Three — Access to the Blockchain Is Centralised

5.3.1 Decentralised ledger, centralised access

The ledger itself is decentralised: thousands of nodes hold copies and no single party can rewrite history. But ordinary consumers, wallets, marketplaces, and applications do not run their own nodes. They reach the blockchain through commercial "RPC" (remote procedure call) gateway providers, a small number of which serve the large majority of wallet and application traffic. MetaMask, the most widely used consumer Ethereum wallet, routes traffic through Infura by default unless the user actively changes the configuration.

5.3.2 Why this matters for ownership

If access is mediated by a few companies, those companies are points at which access can be denied — for legal, regulatory, commercial, or compliance reasons — to a particular jurisdiction or user. This has already occurred: in 2022, Infura restricted access from certain OFAC-sanctioned regions in compliance with US sanctions obligations, with the effect that users of the default MetaMask configuration in those areas could not interact with the Ethereum blockchain through the normal path (see Infura's published compliance statements, available at infura.io). A technically sophisticated user can mitigate this by running their own node or choosing an alternative RPC provider; the ordinary consumer cannot and does not. For that consumer, the practical ability to reach, display, transfer, or sell their own asset is contingent on the continued willingness of an intermediary to serve them.

5.4 Failure Four — The Asset Cannot Exist Without Infrastructure

5.4.1 Important qualification

The first three failures concern the conduct of specific, identifiable parties — artists, platforms, and gateway operators. Failure Four is categorically different: it applies **even if every party behaves perfectly and forever.** It is included here not as a legally cognisable harm in the same sense as the first three failures, but because a court or regulator assessing what a consumer has actually acquired needs to understand the full nature of the thing being sold. A complete consumer-protection analysis requires disclosing not only who can take an asset away, but what the asset fundamentally is.

5.4.2 The dependency on infrastructure

A digital artwork has no independent physical existence. It is not an object; it is a pattern of data. To be perceived at all, it must be reconstructed, in the moment, by a working device drawing electrical power, running functioning software, and — in nearly all real configurations — connected to the internet to fetch the file from wherever it is stored. Remove any of these and the artwork is not merely hard to access; it does not, in any experienceable sense, exist.

This means the value and enjoyment of a digital artwork are permanently tethered to the continued functioning of a vast technical and societal substrate: power grids, internet backbones, data centres, device manufacturers, and software ecosystems. None of this is owned by the buyer, and none of it is guaranteed.

A distinction is worth drawing here, because it is one a defender of NFTs will likely press. Downloaded music files and ebooks also require a device and electricity. Does this mean they are not owned either? The answer is no — and the reason is precisely the distinction this paper is drawing. A downloaded file is *in the buyer's possession*: it sits on their device, under their control, copyable by them independently, and requires no third party's server to remain running. The buyer can play it, copy it, move it, and keep it whether or not the seller still exists. A typical NFT's media file is the opposite: it is not on the buyer's device at all. It is on someone else's server, at a URL the buyer does not control, retrievable only for as long as that server keeps running and that URL keeps resolving. The dependency that matters is not on electricity existing — it is on a specific third party's infrastructure remaining live. That is the dependency of a service, not the dependency of a possession. The legal distinction between owning something and having access to something is precisely the distinction between those two cases.

There is a second and more fundamental distinction that separates digital art from every other category of digital product. When a person buys a piece of software, a film download, or a music track, they are paying for functional utility — for what the product does. The software runs a task. The film tells a story. The music plays. In each case, any working copy restores the full value of the purchase: if the file is lost and redownloaded, nothing of substance is gone. The buyer of a software licence does not care which specific copy of the executable they hold, because one copy is identical to another in every respect that matters.

Digital art and collectibles operate on an entirely different basis. The collector is not paying for what the image *does*. They are paying for what the image *is* — for this specific authenticated work, by this specific artist, with this specific provenance, at this specific edition number. The value is inseparable from uniqueness and authentication. A copy of a Beeple work downloaded from the internet is not worth what a buyer paid for the token, because the copy carries none of the provenance, authentication, or verified scarcity that constituted the thing of value. The collector paid for the blockchain's properties — immutability, verified scarcity, transparent provenance — to be applied to a specific, authenticated instance of the artwork. That is what they were sold.

This is precisely what makes the infrastructure dependency so much more damaging for art than for any other digital product. A software buyer who loses their file loses access to a function they can restore by redownloading. A digital art collector who loses the verifiable connection between their token and the specific authenticated file loses everything they paid for — not merely access to a file, but the authenticated uniqueness that constituted the entire value proposition. The infrastructure dependency does not merely inconvenience the art collector. It destroys the thing they bought.

5.4.3 The contrast with physical art

A physical painting depends on none of this. It can be hung on a wall and enjoyed with nothing more than daylight. In a blackout, an internet outage, a natural disaster, or the failure of the company that sold it, the painting is still there and still gives exactly what it always gave. Its existence and its enjoyment are self-contained. A digital artwork's existence and enjoyment are, by contrast, *contingent and borrowed* — sustained only while the infrastructure around it keeps running. Even the best-engineered NFT — fully on-chain, contract renounced, content permanently stored — still

cannot be looked at during a power cut.

5.4.4 Relevance to disclosure obligations

This is not a doomsday flourish; it is a statement about the nature of the thing being sold. A consumer who pays the price of permanent ownership is entitled to understand that what they have acquired cannot outlast, or even momentarily survive without, infrastructure they do not own and that no seller can promise will always be there. Unlike Failures One through Three, Failure Four cannot be engineered away: it is inherent in what a digital artwork is. For regulators, the significance is disclosure: where the three prior failures could in principle be remedied by better-engineered platforms and contracts, Failure Four means there is a residual infrastructure dependency that must be disclosed regardless.

5.4.5 How the four failures compound

The failures stack. A typical consumer holding is exposed to all four. A diligent buyer who somehow neutralises Failures One and Two (renounced contract, robustly pinned content) still faces Failure Three for everyday access and Failure Four absolutely. There is no combination of buyer diligence, on current market practice, that yields the self-contained, durable control that the word "ownership" promises.

---

6. Sold as a Purchase, Structured as a Subscription

The four failures are technical. Their commercial and legal meaning is captured by a single, decisive observation: **an NFT is sold under the wrong model.** It is marketed and priced as an outright purchase, but it functions as an ongoing, provider-dependent service. This mismatch — and the fact that it is never disclosed — is the heart of the consumer-protection problem.

6.1 The two honest models the market already understands

Commerce already distinguishes cleanly between two kinds of digital product, and consumers understand the distinction:

- **The outright purchase.** A piece of software that installs and runs locally on the user's own computer without requiring ongoing server activation, a music file downloaded to a device, a physical book — these are sold once, for a single price, and thereafter belong to the buyer. They keep working whether or not the seller stays in business, because the thing of value sits with the buyer and depends on no one. This is the model of *ownership*.

- **The subscription / service.** Netflix, Spotify, and Adobe's Creative Cloud are sold as recurring services. The consumer plainly understands that they are paying for *access*, not for an object; that the service requires the internet; that it can change or end; and that everything depends on the provider's continued operation. The terms say so, the billing says so, and the law treats these as services with corresponding consumer protections. This is the model of *access dependent on a provider*.

The defining question is simple: **after I have paid, does the value sit with me, or does it remain with the provider?** If with me, it is a purchase. If with the provider, it is a subscription — whatever it is called.

6.2 NFTs are sold as the first but operate as the second

On the evidence of Section 5, an art NFT plainly belongs in the second category. The valuable part — the artwork — does not sit with the buyer. It remains on the provider's (or a third party's) infrastructure; it can be changed or removed; it can go dark when a company fails; it is reachable only through gateways and only while the internet and power are on. The consumer is, in substance, paying for *continued access to an artwork that someone else hosts and controls* — which is exactly what a subscription is.

Yet the NFT is sold with the form of the first category: a single up-front payment, the vocabulary of "buy" and "own," no recurring bill, and the strong implication of a permanent object that is now the buyer's. The buyer reasonably concludes they have bought an item outright, like a painting or a downloaded file. In reality they have entered something much closer to a Netflix relationship — but one with no monthly invoice to remind them that they are dependent, and no terms telling them so.

6.3 The decisive difference is non-disclosure

The objection to NFTs is **not** that they involve dependency. Subscriptions involve dependency too, and they are perfectly legitimate. The objection is that an NFT carries all the dependency of a subscription while being sold as if it carried none.

- A streaming subscriber *knows* the catalogue can change, that titles leave, that the service needs the internet, and that cancelling ends access. The dependency is disclosed, priced, and understood.
- An NFT buyer is told the opposite of dependency: permanence, immutability, ownership. The dependency on the artist's restraint, the platform's solvency, the pinning service's invoices, the gateway's willingness, and the power grid is rarely, if ever, surfaced clearly at the point of sale, even where a platform's lengthy terms of service contain general risk language a typical consumer will neither see nor understand.

A transaction that has the risk profile of a subscription but the marketing of an outright purchase is, on its face, misleading. The consumer cannot price a risk they are never told exists.

There is a further financial asymmetry that compounds the harm. A subscriber to Netflix or Adobe pays monthly, and if the service closes they lose only future access — they have never overpaid for permanence they did not receive. An NFT buyer paid the entire price, in full, at the moment of purchase, for what they were told was permanent ownership. When the platform closes — as seven major platforms have between 2017 and 2026 — they receive nothing back. They paid the price of a freehold and received the tenure of a tenancy whose landlord has gone out of business. The financial model maximises the buyer's exposure at precisely the moment they have the least information about the risk they are taking.

A third asymmetry operates at the level of execution cost and deserves to be named plainly. When a platform or artist decides to mutate a collection's metadata — calling `setBaseURI` to redirect every token's pointer simultaneously — the cost is one transaction, one gas fee, and one signature. A single actor, paying a few dollars at prevailing gas prices, can alter the state of an entire collection of thousands of tokens in a single block. The consumers affected — each holding a token whose pointer has just been silently redirected — have no equivalent mechanism for collective response. If they wish to individually verify their token's current state, manually recover the original content address, arrange independent IPFS pinning, and document what has changed, each must do so separately, paying individual gas fees and individual storage costs, without coordination and without any guarantee of success. The technology is economically optimised for centralised, one-to-many manipulation: minimal cost to the party with administrative control, distributed across the entire consumer base. It is financially punitive for decentralised, many-to-one consumer recovery: fragmented pinning costs, individual gas fees, and the burden of discovery multiplied across every affected holder. This asymmetry of execution cost is not incidental — it is a structural feature of the architecture that concentrates power in the hands of the controller and fragments remediation among those who bear the harm.

6.4 The protection asymmetry

This mismatch produces a stark asymmetry of protection:

Subscription service	Art NFT	
How it is sold	As a service / access	As an outright pu
Provider dependency	Disclosed; understood at point of sale	Rarely disclosed
Infrastructure requirement	Stated plainly	Rarely stated
Governing terms	Clear, consumer-facing service terms	Marketing of per
Consumer protection	Regulated: cancellation, refund, disclosure rules	Limited; no servi
If the provider disappears	Consumer expected it; paid only periodically	Consumer paid i asset

The consumer in the worse-disclosed, worse-protected position — the NFT buyer — is also the one who has typically paid the *most*, and paid it all up front, for a promise of *permanence*. The party sold the strongest assurance of ownership receives the weakest protection.

6.5 The dilemma: a controlled asset, or a pointless blockchain

When confronted with the fragility above, defenders frequently retreat to: *"It doesn't matter — you can always just download the image and keep it."* This retreat forces a dilemma, and both horns defeat the consumer:

• **Horn one — the asset is controlled.** If the artwork is genuinely the valuable, controlled thing the buyer paid for, then, as Sections 3 and 5 show, the buyer does **not own it**. They hold a receipt for something others control. There is no outright purchase.

• **Horn two — the asset is free.** If the image can simply be downloaded and used freely by anyone, then the blockchain and the token add **nothing of value**. The buyer has paid a large sum for a database entry pointing at a file that is free to the whole world. One could simply sell the image — as countless royalty-free image libraries already do — for a fraction of the price.

A sophisticated defender may attempt a third position: that the token has independent value as a provenance record — a receipt confirming authenticity — regardless of where the image lives or whether anyone can download it. This position is worth taking seriously, because it is the most coherent defence available. But examined closely, it does not rescue the NFT; it destroys it from a different direction.

For a provenance record to function as such, it must be cryptographically bound to the specific file it certifies. Without that binding — which requires a correctly populated integrity hash — the token certifies only that a URL once existed, not that any particular file was ever associated with it. In the overwhelming majority of NFTs on the market, that binding does not exist. The `image_hash` field — designed to create exactly this cryptographic link — is absent, blank, or set to the literal placeholder string `"none"`. This is the normal condition of the market, documented in the illustrative case in Section 4 and reproducible across collections.

Where a real `image_hash` is present, it does establish something of genuine value: a verifiable, tamper-evident link between the token and a specific sequence of bytes. A court could use that hash to establish that a particular file was the one originally associated with the token, and to adjudicate disputes about whether the current file matches the original. In this narrow sense, a correctly populated hash successfully establishes authenticity and historical linkage to the transaction — and this paper does not dispute that.

What a hash cannot establish — and what defenders of the provenance position frequently elide — is exclusivity of possession or structural control. Consider the contrast with physical real estate. A land registry deed grants the owner the legal right to exclude others from the land: trespassers can be removed, access can be denied, and the exclusive physical use of that space is the defining right the deed confers. This exclusivity is meaningful precisely because land cannot be copied — there is one plot, and the deed secures sole control over it. An NFT with an integrity hash does the exact opposite: it confirms you hold a deed, while the legal and technical framework simultaneously permits the rest of the world to copy, store, distribute, and occupy the identical digital space without recourse. The hash tells you your copy matches the original. It gives you no mechanism to prevent anyone else from holding an equally valid matching copy.

A cryptographic hash is a fingerprint of a file's *content*, not of any particular instance of that content. The hash function is deterministic: the same input always produces the same output. Anyone who holds an identical copy of the file produces an identical hash. The token says "this hash value belongs with this token." Every copy produces that same value. The hash cannot tell you which of the millions of potential holders of the same file is the legitimate owner, because from the hash's

perspective they are indistinguishable.

The provenance position therefore succeeds only in establishing one thing: that the file you are looking at today matches the file associated with the original transaction. It cannot establish that you are the exclusive owner. It cannot establish structural control. And it cannot establish any of the rights that property ownership ordinarily confers. What the NFT industry sold as ownership is, at best, an authenticated transaction record for a file that anyone may freely hold. That is a meaningful thing — but it is not what was sold, and it is not what consumers paid for.

The third position therefore does not escape the dilemma — it collapses entirely into Horn Two. Furthermore, as Section 3.7 establishes, the provenance chain the token is supposed to represent is itself fragile in two independent ways: the blockchain cannot verify that the minting wallet belonged to the claimed artist, and loss of wallet access by any party in the chain permanently severs the proof of ownership with no legal remedy.

There is a final dimension to the Horn Two collapse that has not yet been named. When a platform fails and a consumer is left with an on-chain token pointing to a dead URL, they face a double vacuum of ownership. On the technical side, the token points to nothing — the artwork is inaccessible. If they resort to downloading a copy of the image from a cached source or a secondary marketplace, they have resolved only the technical problem, and only temporarily. On the legal side, they hold a file to which they have no intellectual property rights. As Section 3.6 establishes, the purchase of an NFT does not transfer copyright in the underlying work absent an explicit written agreement. The copyright remains with the artist. The consumer who downloads the image cannot legally display it in a commercial context, exhibit it publicly, reproduce it, or monetise it in any form without the artist's permission — permission they have no mechanism to obtain from an artist they may not be able to locate, under a token that no longer functions as evidence of any transaction with that artist. They hold a file they cannot exploit, under a token that points nowhere, with no copyright and no functioning provenance record. This is the practical outcome of Horn Two: not "you can always download the image," but "you can always download an image you have no right to use, that you cannot prove you legitimately acquired, attached to a token that no longer connects to anything."

One apparent exception to the Double Vacuum deserves direct address. A number of prominent NFT collections — including Nouns and Goblintown — are released under Creative Commons Zero (CC0) licences, under which the creator dedicates the work to the public domain, waiving or relinquishing their copyrights and related legal rights to the maximum extent permitted by applicable law. A defender of such a collection may argue that the legal vacuum described above does not apply: under CC0, any holder of the downloaded file has full, unconditional legal right to display, modify, and commercially exploit it without restriction. This is factually correct as far as it goes. However, rather than rescuing the Horn Two position, a CC0 licence accelerates its collapse. The marketing of CC0 collections as scarce, exclusively owned, premium-priced collectibles is precisely contradicted by the licence. If the work is legally free for the entire world to exploit without any restriction whatsoever, the token's premium pricing as a rare or exclusive digital asset is a commercial paradox. The consumer has paid a significant sum for exclusive ownership of an asset whose creator simultaneously and irrevocably gave it to the entire world for free. The legal vacuum

of the downloaded file is resolved — but only by eliminating the very exclusivity that justified the price. Under CC0, the Horn Two outcome is not softened; it is completed at the point of minting.

On no reading of the technology as it actually exists in the market does the consumer end up holding a verifiable, exclusive claim to a specific, identifiable artwork.

---

7. Scale and Scope: How Many Consumers Are Affected

The failures described in this paper are not exceptions within the market. They are its default condition.

7.1 Market size and consumer exposure

Global NFT sales across all categories exceeded US$25 billion at their peak in 2021 (DappRadar annual market report). Art and collectibles collectively represented the largest share of that market by volume. The Christie's sale of Beeple's *Everydays: The First 5,000 Days* at US$69.3 million in March 2021 — for which MakersPlace minted the NFT — drew a new wave of consumer buyers into the market who understood themselves to be purchasing a permanent, ownable digital artwork. NFT platforms collectively hosted millions of tokens. The overwhelming majority of those tokens pointed to assets stored on private company servers or unpinned IPFS, under contracts whose ownership had not been renounced. The structural failures this paper describes applied to virtually all of them — not as a theoretical risk, but as the live condition of every purchase made.

7.2 Platform failures: a quantified record

By 2026, the contraction of the market had produced a documented record of platform insolvencies and closures, each resulting in hosted artwork being placed at risk. The full record — with dates, reported figures, and what each closure meant for hosted works — is set out in the table in Section 8.1. Between them, the platforms documented there hosted a significant fraction of the consumer NFT art market. This is not a list of edge cases. It is a list of mainstream, well-funded platforms operating under the same structural architecture this paper describes.

7.3 The typical consumer cannot protect themselves

The means available to a consumer to detect these risks — reading verified smart-contract source code on a block explorer, inspecting HTTP response headers, checking IPFS pinning status, understanding RPC gateway configuration — are technical skills far beyond what can be expected of an ordinary buyer. A consumer purchasing a work at auction, or through a gallery's digital platform, has no realistic way to discover that the contract has not been renounced, that the artwork sits on a company server, or that the platform offers no custodial segregation. They rely on the marketing, and the marketing says they own the art permanently.

The asymmetry of information is not incidental; it is structural. It is the reason a regulatory response — rather than case-by-case consumer litigation — is the appropriate remedy.

8. The Pattern Is Established, Not Hypothetical

Section 7 catalogued platforms by the scale of what was lost when they closed. This section looks at those same closures differently: not as a count of incidents, but as a pattern of conduct — asking what they had in common, and what that tells us about how the market is built.

8.1 Historical record of platform closures

Between 2017 and 2026, numerous NFT platforms shut down, were acquired, or entered wind-down, and a recurring outcome was that tokens survived on the blockchain while the hosted artwork disappeared. The figures below are drawn from public reporting and the companies' own announcements; they are presented as publicly reported figures and estimates rather than independently audited counts, and each is checkable against the cited public statements.

Platform	Outcome	What was reported
Ascribe / Digital Objects	Pivoted / shut down (c. 2017–2018)	Many early works reported as permanently lost after servers were taken offline; not all works affected
Editional	Shut down (c. 2019)	Reportedly 100,000+ NFTs with metadata on company servers
FTX NFT Marketplace	Exchange collapsed (Nov 2022)	Hosted artwork observed redirecting to a bankruptcy/restructuring notice
Recur	Shut down (2023)	Domain reported as no longer resolving
MakersPlace	Shut down (Jan 2025)	Minted the NFT for the Christie's US$69.3m Beeple "Everydays" auction; announced closure 16 January 2025 (MakersPlace, "MakersPlace Announces Market Exit," January 2025); NFT transfer deadline imposed for June 2025
Foundation	Permanently closed (Apr 2026)	Ownership transferred to Blackdove (announced 27 January 2026); deal collapsed by mid-April 2026 (Kayvon Tehranian, open letter on X, 15–16 April 2026; Foundation/@foundation on X, 16 April 2026); US$230m+ in lifetime primary sales confirmed in founder's January 2026 letter; infrastructure shut down

Platform	Outcome	What was reported
Nifty Gateway	Closed (Apr 2026)	Closure announced 24 January 2026 (Gemini, "Announcing Nifty Gateway's Closure," gemini.com, 23 January 2026); reportedly home to an estimated 650,000 NFTs; platform officially closed 23 April 2026; legacy metadata for pre-2022 NFTs server-bound per platform's own disclosure

The pattern is consistent: a platform launches, hosts metadata on its own servers, the market shifts, funding dries up, the company shuts down, and the tokens are left pointing to URLs that fail.

8.2 The "you do not own anything" demonstration

In March 2021, an artist working as "neitherconfirm" listed 26 NFTs for sale on OpenSea and then, while listings were still active, replaced every artwork — at the server the artist controlled — with pictures of rugs. The on-chain `tokenURI` never changed; the content at that URL did. Every marketplace and wallet then displayed a rug. The artist's stated point was exact, in their own words: *"As long as the value of your artwork is reliable on a central service you do not own anything."*

8.3 The exchange-collapse case

After the FTX collapse in November 2022, NFTs whose metadata pointed to FTX-controlled domains were observed resolving to a corporate restructuring page. Holders kept their tokens; what those tokens displayed became a bankruptcy notice. The token survived; the art did not.

8.4 Permanently lost early works

Some of the earliest and most historically significant crypto-artworks, minted on platforms that shut down in 2017–2018, are now considered permanently lost: the tokens persist on an immutable blockchain, but the art was stored on temporary servers that no longer exist. Many works tokenised precisely to achieve permanent ownership were among the first to be permanently lost.

8.5 The counter-example that proves the rule

When the Tezos-based platform Hic et Nunc was shut down without warning by its founder in November 2021, the vast majority of its artworks **survived** in accessible form. This was not because the blockchain protected them — the ledger behaved identically to every case above — but because the media had been stored on IPFS using native content addresses, and the contracts remained on-chain. Community mirror sites reconnected to the same IPFS content within hours, and ClubNFT and other organisations in the community coordinated to pin the content across multiple nodes. It should be noted that this was also partially a front-end failure: ownership and metadata remained on-chain throughout. Nonetheless, the determinant of survival was unambiguous — **where the art was stored**, not that it was on a blockchain. Survival turned on storage architecture, which the

consumer does not choose or control at point of purchase.

9. Digital Versus Physical Asset Ownership

Dimension	Physical artwork	Digital art NFT (typical)
What the buyer holds	The object itself	A token and a changeable pointer
Who can alter the work after sale	No one — alteration is forgery, and detectable	Artist (via contract) and platform (via server), often without trace
Who can make the work disappear	Only through theft or physical destruction	Any host, registrar, cloud provider, pinning service, or artist — by act or omission the owner cannot prevent
What diligence protects the owner	Careful handling; security against theft	Little to nothing within the owner's power
Third-party solvency dependency	None, once delivered	Continuous and indefinite
Ability to access/display	Inherent in possession	Mediated by centralised gateways
Usable without infrastructure	Yes — needs only daylight	No — needs power, device, software, and usually the internet
Survives blackout / disaster	Yes	No
Proof of ownership if access is lost	Established through receipts, insurance, legal records, court process	Requires signing with the wallet's private key; if the seed phrase is lost, proof is permanently impossible
Verification of seller's right to sell	Provenance records, auction history, expert authentication	Blockchain confirms token transfer; cannot verify the minting wallet belonged to the claimed artist or that the minter had any right to create the work
Third-party claim via downloaded copy	No — copying does not create title	Effectively yes — no mechanism distinguishes the buyer's copy from any other without a cryptographic binding
Resale and transfer	Hand over object, sign receipt; title passes on delivery	Custodial: internal database update, token never moves on-chain. Self-custodied: requires wallet coordination and gas fees. In neither case does the artwork transfer
Inheritance	Title passes by will, probate, or succession law; no technical access required	Token permanently locked if seed phrase is not passed on; no court process can recover it
Commercial model	Outright purchase	Sold as a purchase; functions as a subscription

With a physical piece, a careful and honest owner who guards against theft and damage can keep their property for a lifetime and pass it on; the decisive factors are within their control. With a typical digital artwork, the buyer can perform every step of diligence available to them and still lose the asset, or control of it, or access to it, through the conduct of others — or simply because the lights went out. **The digital "owner" bears the language and the price of ownership without the substance of it.**

---

10. Consumer Harm and the Gap Between Marketing and Reality

The harm that flows from the failures described above is not hypothetical, and it does not require anyone to have acted in bad faith. It is the predictable consequence of selling one thing — an outright, permanent purchase — while delivering another: a dependency-laden service with no disclosure, no terms, and no protection equivalent to what even the cheapest streaming subscription provides.

The specific forms that harm takes are worth naming plainly. Consumers are misled about permanence: they are told they "own" something that the artist can redirect, the platform can modify, and the infrastructure can render invisible, all without their knowledge and often without any trace. They are misled about the commercial model: they pay a single price, in full, up front, for what functions as a provider-dependent service — a Netflix relationship without the monthly invoice and without the terms that would tell them so. When a platform winds down, "in perpetuity" hosting commitments turn out to be unenforceable corporate promises from businesses that have already decided to close. Consumers in custodial arrangements may never have received the token they think they hold; their "ownership" is a database entry that the platform can modify or delete. And the artwork itself can be changed after sale — its content silently swapped at the server level, with no on-chain record of the substitution — which is not a sale at all in any legal sense of the word.

What makes all of this structural rather than incidental is the last point: none of it requires malice. A well-intentioned artist and a solvent, honest platform can still, simply by going out of business years later, strand everything a consumer believed they owned. That is not a dispute about conduct. It is a dispute about what was sold — and what the law should say about selling it that way.

The asymmetry of information that enables this is also structural. The artist and platform hold every technical key: the contract owner function, the server credentials, the pinning account. The buyer holds a receipt. Closing this asymmetry through litigation, case by case, would be slow and inadequate. It calls for a regulatory response that sets the terms of what must be disclosed before the purchase is made.

10.1 The insolvency gap: custodial NFTs are not segregated client assets

One specific dimension of consumer harm warrants focused attention because it arises from an established gap in existing law rather than from the NFT industry's conduct alone.

In most jurisdictions, when a custodial platform becomes insolvent, assets held in the platform's accounts are treated as assets of the insolvent estate unless they can be identified as client property held on trust or under a segregation obligation. This distinction is decisive for consumers. A client whose assets are properly segregated recovers those specific assets from the insolvency — they are not creditors competing for a share of whatever remains. A client whose assets are pooled in the estate's accounts becomes an unsecured creditor, receiving cents on the pound (or dollar) after secured creditors and administration costs are satisfied.

The FTX collapse in November 2022 illustrated this gap in the crypto context with precision. Customer funds and assets held on FTX's platform were not legally segregated from the company's own assets. Customers became unsecured creditors. Years of legal proceedings followed, with recoveries far below the assets customers believed they held.

Custodial NFT platforms present an identical structural problem. Where a platform holds tokens in an omnibus wallet on behalf of consumers — the model documented in Section 4 in the context of the Beeple Spring Collection on Nifty Gateway — those tokens are legally held in the platform's name, not the consumer's. If the platform becomes insolvent, the consumer's claim to those tokens is not a property claim but a contractual claim against the estate. The consumer is not retrieving their own property; they are asserting a debt. In practice, given the administrative costs of NFT marketplace insolvencies and the illiquid, highly volatile nature of the assets, unsecured creditors in this position typically recover little or nothing.

The UK Law Commission's 2023 digital assets report acknowledged this gap specifically, noting that existing trust and insolvency frameworks were not designed with digital asset custody in mind and that legislative intervention may be required to protect customers of digital asset custodians. No major jurisdiction has yet enacted such legislation. In the interim, consumers who hold NFTs on custodial platforms are exposed to an insolvency risk that the marketing of those platforms — which presents the consumer as the "owner" of their collection — does not disclose. Recommendation R5 addresses this in part by requiring custodial disclosure; the deeper fix requires insolvency legislation that mandates segregation of customer digital assets as a condition of operating a custodial NFT platform.

---

11. Practical Recommendations

The aim is to close the gap between the marketing of ownership and its technical reality, without prohibiting the technology. The recommendations are deliberately concrete and are framed as principles applicable to any jurisdiction; the precise legislative or regulatory vehicle will vary by legal system.

11.1 For Regulators and Consumer-Protection Authorities

Preliminary note: No jurisdiction has yet authoritatively applied its consumer-protection framework to NFT transactions in terms that address the structural failures described above. The

recommendations below propose a prospective framework, not a statement of existing law. They are offered as a starting point for regulators who are determining what obligations should apply and how existing consumer-protection principles extend to this market.

Seven recommendations follow. The first three — disclosure, honest marketing, and service-appropriate classification — are the minimum required to close the gap this paper has described. The remaining four address the specific mechanics of storage, custody, access, and attestation that those three principles must reach to be effective in practice.

R1 — A mandatory, standardised point-of-sale "Ownership Label." Every NFT offered to consumers should carry, before purchase, a short standardised label that answers plain questions with plain answers:

Disclosure question	Required answer
Where is the artwork stored?	On-chain / Arweave (permanent endowment) / IPFS with verified pinning contract / IPFS unverified / Private servers
Can the artist or platform change or remove the artwork after sale?	YES / NO
Has contract ownership been permanently renounced?	YES / NO
Is there an integrity hash linking the token to this exact file?	YES / NO (placeholder such as "none" counts as NO)
Do you receive the token in your own wallet, or does the platform hold it?	Self-custody / Platform-custodial
Who funds long-term storage, and for how long?	[Named party and term]

The effect is to convert the entire technical analysis of this paper into a single signal a consumer can read in seconds — the equivalent of a nutrition label or an energy-efficiency rating. It does not require the buyer to understand blockchain architecture. It requires the seller to be honest about what they are selling.

Note on field independence: The fields in the Ownership Label are independent variables. A favourable answer in one field does not guarantee a favourable answer in any other. Most critically: a collection that correctly discloses permanent on-chain or Arweave storage may simultaneously disclose that the artist or platform retains the power to change or remove the artwork — because the storage layer and the contract control layer are separate architectural components. A token pointing to an Arweave-stored file can still have its `tokenURI` redirected by an unrenounced contract owner to point elsewhere entirely. Consumers and regulators should read all fields together, not treat any single field as sufficient assurance of asset integrity.

Enforcement mechanism: Because smart contracts can be deployed pseudonymously from any jurisdiction and interacted with directly through a blockchain node, regulators cannot practically

mandate compliance at the protocol level. The enforcement target must be the centralised interface layer: consumer-facing marketplaces, wallet extensions, and platform front-ends. Regulators can require that licensed or registered digital asset marketplaces refuse to display, list, or facilitate transactions for collections that do not serve a compliant Ownership Label through their API or user interface. Similarly, wallet providers operating under financial licences can be required to surface the label before confirming a purchase transaction. This approach mirrors the regulatory architecture already applied to financial product disclosures: the disclosure obligation falls on the intermediary with a consumer-facing relationship, not on the underlying instrument itself.

One limitation of this approach warrants explicit acknowledgement. Decentralised, immutable frontends — interfaces hosted via IPFS or accessed through Ethereum Name Service domains, modelled on open-source client deployments such as Uniswap's — exist outside the reach of licensed gateway regulation and cannot be targeted through this mechanism. A sufficiently motivated participant could interact with a non-compliant smart contract directly or through such an interface, bypassing any label requirement entirely. This paper does not propose that the centralised-interface enforcement mechanism eliminates this pathway. It proposes that targeting centralised frontends cuts off the mainstream retail pipeline — the entry point through which the overwhelming majority of consumer-protection harm in this paper actually occurs. Peer-to-peer and dApp-native interactions are conducted almost exclusively by technically sophisticated participants who are not the consumer demographic this framework is designed to protect. The goal of R1 is to close the harm at scale, not to achieve universal coverage of every possible interaction pathway.

Cross-border jurisdictional reach: A related limitation is regulatory arbitrage. If domestic regulators enforce strict Ownership Label requirements on licensed gateways, non-compliant collections may shift primary drops to marketplaces and frontends operating from unregulated jurisdictions or sovereign tax havens. Mainstream consumers can access these venues via VPN or decentralised frontend interfaces. Domestic enforcement cannot prevent a consumer from actively seeking out non-compliant international venues. It can, however, establish a clear and enforceable legal line for domestic liability. A foreign platform that actively targets or accepts capital from domestic retail consumers without surfacing the mandatory R1 label — through localised advertising, geo-targeted marketing, domestic payment rail acceptance, or domestic language interfaces — provides domestic consumer-protection authorities with clear grounds to take enforcement action. Available tools include: enforcement actions against domestic payment processors and banking intermediaries that facilitate transactions with the non-compliant platform; asset seizures where the platform or its principals hold domestic assets; and mandated ISP blockades of the consumer-facing pipeline within the domestic jurisdiction. This is the established model for extraterritorial consumer protection enforcement — analogous to the GDPR's application to any entity processing EU citizens' data regardless of where the entity is incorporated. Domestic enforcement does not achieve universal coverage; it achieves domestic accountability and raises the compliance cost for any platform that wishes to access a regulated market's consumer base.

Dynamic compliance monitoring — an operational mitigation, not an architectural cure: The point-of-sale label addresses conditions at the time of purchase. It does not address changes that occur post-sale — most critically, a change to a collection's base URI after consumers have already

bought tokens. To make the Ownership Label persistent rather than a one-time snapshot, consumer-facing wallet extensions and marketplace interfaces should be required to implement a continuous compliance monitor: an open-source script that queries the relevant contract's current state — owner address, base URI, and renunciation status — at the time the asset is displayed and compares it against the state recorded at the original point of sale. The monitoring script requires no privileged access — all the relevant state is publicly readable from the blockchain — and its open-source specification allows independent verification that it has not been tampered with.

Alert thresholds must be tier-ranked to prevent alert fatigue and to provide consumers and regulators with a calibrated signal. A single undifferentiated "warning" applied to all contract state changes — including routine administrative transfers such as a platform updating its multi-sig signers or completing a corporate acquisition — would desensitise holders to genuine asset-integrity events. The recommended tier structure is:

- **Yellow — "Management State Change":** triggered when the contract owner address changes to an address that is not pre-registered as part of the platform's verified corporate vault registry, without a corresponding change to the base URI. Routine administrative key rotations — such as a platform cycling between its own multi-sig wallets, cold storage vaults, and operational hot wallets for security compliance — should be exempted from the Yellow threshold provided the destination address has been cryptographically pre-linked and publicly registered as part of an identity-verified platform registry prior to the transfer. Transfers to unverified pseudonymous addresses, or to any address outside the registered vault set, trigger Yellow regardless of whether the base URI has changed. This distinction preserves the signal value of the alert: it flags genuine changes in control to an unknown or unregistered party, not routine internal key-management lifecycle events that generate noise without indicating consumer risk.
- **Red — "Asset Integrity Compromised":** triggered when the base URI string itself changes, when the underlying bytecode proxy target changes (indicating a logic upgrade), or when contract ownership transfers to an unverified address simultaneously with a metadata change. This indicates that the asset the holder purchased may no longer be the asset the token currently represents. Immediate action — verifying the current token URI and its content against the original sale record — is warranted.

It is important to frame this mechanism accurately. Dynamic compliance monitoring is an operational patch applied at the interface layer — it is not an architectural cure for the structural problem this paper identifies. A reader who has followed the argument will notice the self-referential limitation: this paper argues at length that consumers cannot be expected to run independent blockchain queries or navigate Etherscan, yet the post-sale safety net described here depends on third-party commercial wallet extensions — companies such as ConsenSys operating MetaMask — voluntarily implementing, executing, and maintaining an unmonetised monitoring script on client-side hardware. If a wallet provider encounters a bug, drops support for the script, faces an RPC outage, or simply deprioritises the feature, the dynamic label fails — and fails silently. The consumer receives no indication that their protection has lapsed. This is precisely the architecture of dependency this paper argues against. The dynamic compliance monitor is necessary precisely because the underlying protocol permits hostile post-sale mutations — it transfers the burden of warning to the consumer-facing pipeline because the asset-level architecture imposes no constraint on mutation.

That is not a solution. It is a disclosure of why a solution at the architectural level — permanent renunciation, immutable URIs, on-chain storage — is the only genuine remedy. The monitor buys time and visibility. It does not fix the building.

Mempool front-running vulnerability: A further technical limitation applies specifically to the pre-sale compliance check — the state verification performed by the monitor at the moment a consumer's wallet presents the transaction for signing. This check reads contract state from a public RPC node at a single point in time. Between that snapshot and the transaction settling on-chain, a malicious contract owner can exploit a well-documented blockchain vulnerability: asymmetric front-running, also known as a sandwich attack. By broadcasting a `setBaseURI` call with a higher gas fee immediately after observing a high-value consumer transaction broadcast to the public mempool, the attacker's state-mutation transaction can be mined into the block ahead of the consumer's purchase. The consumer's wallet UI displays a compliant label based on the state milliseconds earlier; by the time their transaction settles, they have purchased a mutated or redirected asset.

For high-value consumer transactions, the interface layer should be specified to route transactions through private RPC relayers — such as Flashbots Protect or MEV-share architectures — that bypass the public mempool entirely and submit transactions directly to block builders. This eliminates the asymmetric front-running window: because the consumer's transaction intent is never exposed to the public mempool, a malicious actor cannot observe it and race to mutate state ahead of it.

Private RPC relayers do not, however, eliminate all race conditions. If a contract owner independently calls `setBaseURI` before the consumer submits their transaction — not in response to observing a pending transaction, but as a unilateral act occurring earlier in time — the mutation will settle on-chain before the consumer's purchase regardless of whether a private relayer is used. No relay architecture can protect against a state change that has already been committed to the chain. The complete mitigation for this standard race condition requires the consumer's purchase transaction itself to contain an explicit cryptographic state assertion: a conditional checkpoint inside the purchase execution function that verifies a hash of the current base URI at the moment of settlement and causes the transaction to revert automatically if that hash does not match the state the consumer verified at signing. If the contract owner has already mutated the base URI, the hash will not match, the transaction will revert, the consumer's funds will be returned, and the purchase will not settle.

This requirement places a specific obligation on marketplace architecture that does not exist in current dominant infrastructure. The leading immutable marketplace execution protocols — including OpenSea's Seaport and Blur's native order-matching contracts — are deployed on-chain as immutable smart contracts that cannot be modified by the marketplace operator to support arbitrary state checks. The enforcement pathway is therefore not at the smart contract level but at the frontend web interface layer: marketplace operators must update their client-side JavaScript wallet payload generation to wrap transactions in compliant execution logic — evaluating the cryptographic state assertion and constructing a compliant transaction payload — before broadcasting to block builders. This is an enforceable obligation because the frontend interface is under the marketplace

operator's direct control, unlike the immutable on-chain matching contracts. Regulators requiring this protection should specify it as a frontend interface obligation, not a protocol-level requirement, and condition marketplace licences on demonstrable frontend compliance verified through interface audits.

R2 — Truth-in-advertising restrictions. Prohibit the unqualified use of "own," "sale," and "permanent" where the asset is centrally hosted, mutable, or custodially held. Where those conditions exist, require a plain-language qualifier stating what the buyer actually receives and the risks to its continued existence.

R3 — Classify dependency-bearing NFTs under service / subscription consumer law. Where an NFT's value depends on the seller's or a third party's continued hosting, operation, or good faith, treat the transaction, for consumer-protection purposes, as the ongoing service it functionally is — attracting the same disclosure, fairness, and continuity obligations that apply to subscription services. The Ownership Label required by R1 provides the operative test: where any field in that label indicates dependency — private server storage, a live `setBaseURI`, platform-custodial holding, or unfunded storage — R3's classification applies. A product that carries subscription-like dependency should not escape subscription-like protection merely because it is sold for a single up-front price and labelled a "purchase."

Non-displacement note: Classifying a transaction as a consumer service for the purposes of this recommendation does not preclude, displace, or override its classification as a financial instrument, investment contract, or security under applicable financial regulation. Consumer-protection law and securities law address different harms and operate in parallel. A regulator or court applying R3 should treat it as supplementing, not substituting for, any financial regulatory analysis that may independently apply to the same transaction.

R4 — Storage-permanence and continuity obligations. Require platforms to maintain, and to disclose, a credible asset-continuity plan — for example, migration of metadata and media to decentralised, content-addressed storage (IPFS with funded multi-year pinning, or Arweave) with a named, funded custodian of last resort. A bare "indefinite hosting" promise unbacked by a technical guarantee should not satisfy this obligation.

R5 — Custodial-holding transparency and segregation. Where a platform holds tokens custodially, require clear disclosure that the consumer does not hold the token on-chain, plus rules on segregation of customer assets and a defined process for what happens to holdings on insolvency or wind-down (including a guaranteed withdrawal window).

R6 — Access-resilience disclosure. Require disclosure that everyday access typically depends on third-party gateway providers who may restrict access, and that the asset cannot be displayed without internet, power, and functioning software; signpost consumers to self-custody and independent-access options.

R7 — A self-executing pre-sale technical attestation via automated compliance scanning. Require that every NFT collection offered to consumers be accompanied by a machine-generated

compliance report, produced by an open-source, automated on-chain analysis tool at the time of contract deployment. Tools of this type already exist in the smart contract security domain — static analysis frameworks such as Slither and Mythril can programmatically parse contract bytecode and source code to identify the presence and accessibility of administrative functions including `setBaseURI`, proxy upgrade patterns, and owner-controlled mint functions. A compliance scanner built on this model could automatically determine and report: whether the contract contains a mutable base URI function; whether contract ownership has been renounced; whether the token URI resolves to content-addressed storage or a private domain; whether an integrity hash field is populated; whether active, verifiable on-chain pinning exists (such as a Filecoin storage deal or Arweave endowment) rather than passive IPFS propagation; and whether the contract implements a proxy upgrade pattern. The platform must link this verifiable, machine-generated report to their consumer-facing point of sale. Regulators do not audit the bytecode; they audit whether the report is present, current, and matches what the point of sale discloses. Liability attaches if the seller's disclosures conflict with the machine-generated report. This approach removes the verification burden from underfunded regulatory bodies and places it on automated tooling that cannot be deceived by self-reporting.

State mutation caveat: Static analysis tools read contract state and function signatures at the moment of analysis and cannot exhaustively detect all conditional execution branches that depend on runtime state. A malicious contract can pass static analysis cleanly at deployment and subsequently activate hidden administrative functions after a specific block number has elapsed, after receiving a signal from an external oracle, or via a `delegatecall` to an upgradeable proxy that static analysis cannot fully trace. To mitigate this attack vector, the compliance scanner must be specified to flag — and the point-of-sale disclosure must affirmatively identify — any contract containing: conditional execution structures whose activation depends on block numbers, timestamps, or external triggers; dependency on external oracles or off-chain data sources for core metadata properties; unrenounced `delegatecall` logic or external target calls that could mutate contract behaviour post-mint; or proxy upgrade patterns of any kind including Transparent Proxy and Diamond architectures. Contracts containing any of these features must be disclosed as carrying unverifiable Failure One exposure regardless of their state at the time of scanning. A clean scan result for a contract with conditional mutation logic is not a clean result — it is an incomplete one.

11.2 For Platforms, Marketplaces, and Artists

P1 — Renounce contract ownership. The only technical state that fully eliminates Failure One is permanent, irrevocable renunciation of contract ownership — transferring the owner role to an address no one controls (the zero address) — or, equivalently, a contract whose metadata URI is hard-coded as an immutable constant at deployment with no administrative function capable of changing it. In either configuration, no party can redirect the token's pointer, and the structural control that constitutes Failure One is permanently removed.

Multi-signature arrangements and time-locked administrative processes are not equivalent to renunciation and should not be presented as such. A multi-sig contract shifts unilateral control from a single wallet to a small committee of wallets, but the structural trust requirement remains: if signers

collude, are compromised, or are subject to legal compulsion, the control can still be exercised. Proxy upgrade patterns — including Transparent Proxy and Diamond proxy architectures — are materially worse: they can silently modify the contract's logic itself, not merely its metadata pointer, and introduce upgrade vectors that compound rather than mitigate Failure One. These patterns should be disclosed as carrying full Failure One exposure, not presented as safety measures.

Where ongoing administrative access is genuinely required — for example, to update royalty recipients or administrative addresses — it should be separated from metadata control by architecture: the metadata URI should be locked immutably at deployment while other administrative functions are placed behind time-locked, publicly visible multi-signature governance. Under no circumstance should metadata mutability be presented to consumers as a feature equivalent in safety to renunciation.

P2 — Store the asset where it cannot be quietly changed or lost: on-chain for small works; otherwise on content-addressed storage (IPFS or Arweave) referenced by the **native content address**, never by a single company's gateway URL.

P3 — Fund permanence explicitly, with a sustainable and enforceable economic model. The question of who bears the cost of permanent storage is not trivial. An artist who mints a work, sells it for $100, and has no further connection to subsequent resales is not a sustainable candidate for indefinite storage liability — particularly where a work later trades for tens of thousands of dollars on a secondary market in which the original creator receives little or no royalty. Placing that liability on the original minter alone is economically unsustainable for independent creators and creates a permanent financial obligation disconnected from the asset's ongoing value.

The sustainable solution is to embed storage funding in the smart contract's transactional architecture rather than relying on the original minter's goodwill. For primary sales, this is architecturally straightforward: a fixed percentage of the primary sale proceeds, routed automatically by the contract at the time of mint, should be directed to a pre-paid perpetual storage service such as Arweave or a contract-controlled storage endowment. Primary sale routing is under the contract's direct control and is not subject to marketplace discretion.

Secondary sales present a materially different problem. Since 2022–2023, the dominant secondary marketplaces — Blur and OpenSea following Blur's market dominance — have moved to off-chain order books and optional royalty models that bypass on-chain royalty enforcement entirely. A trade executed through these wrappers routes zero to any on-chain storage fund, regardless of what the contract specifies under EIP-2981. The "Royalty Wars" of that period reduced secondary royalty enforcement from a structural guarantee to a courtesy subject to marketplace policy. Any P3 implementation that relies on secondary fee routing for ongoing storage viability must therefore also implement structural transfer restrictions: specifically, contract-level transfer blocks against known zero-royalty marketplace wrappers, or strict EIP-2981 royalty enforcement architectures that condition token transferability on royalty compliance. If a collection's token contract lacks these enforcements — as the R7 compliance scanner should be specified to detect — the collection's long-term storage must be flagged as unfunded and dependent on primary-sale endowment alone or on the minter's voluntary contribution. A bare assumption that secondary sales will fund storage,

without verified enforcement architecture, should not satisfy this obligation.

This recommendation introduces a structural trade-off that warrants open acknowledgement. This paper's foundational argument is that NFTs fail to deliver the rights of true ownership to consumers — including the right to freely dispose of an asset through any marketplace of the owner's choosing. Contract-level transfer restrictions that dictate which platforms a consumer may use to sell their token directly constrain alienability — one of the core property rights the paper argues consumers were promised and did not receive. An intellectual adversary will note the apparent contradiction: the paper condemns the industry for failing to deliver true ownership, then proposes a solution that strips consumers of free transferability. That tension is real and should not be obscured. The correct framing is that mandating transfer restrictions to preserve storage funding is a defensive necessity imposed by the underlying architecture — a digital artwork cannot structurally mirror a self-contained physical object without constraining the open-market properties of the token that represents it. A physical painting can be sold through any auction house without routing any fee to a storage endowment, because the painting physically exists regardless of how it is sold. A digital artwork dependent on an ongoing storage fund cannot make the same guarantee unless the funding mechanism is protected from circumvention. The trade-off between alienability and asset permanence is not a flaw in the recommendation; it is further evidence of the paper's core thesis — that digital art ownership cannot replicate the structural properties of physical property without architectural constraints that have no equivalent in the physical world.

P4 — Populate a real integrity hash of every media file in the metadata, so any holder can independently verify the file has not changed. Never ship `"none"`.

P5 — Default to self-custody. Deliver tokens to the buyer's own wallet; where custody is offered, segregate assets and guarantee withdrawal.

P6 — Publish a wind-down commitment in advance: on shutdown, migrate assets to decentralised storage and hand holders the native content addresses.

P7 — Plan for artist death and entity dissolution. Where a contract's owner is an individual artist's wallet, establish a documented succession plan — a multi-signature arrangement or a time-locked transfer — so that the contract does not become permanently frozen if the artist dies or loses access to their wallet. Holders should not lose all ability to administer their tokens because of events entirely outside their control.

11.3 For Consumers and Their Advisers

These checks are presented for completeness and for advisers acting on behalf of consumer clients. They are not offered as a substitute for the regulatory response this paper argues is necessary: the fact that a technically informed buyer could in theory perform these steps does not place the burden of disclosure on the buyer, any more than the existence of food chemistry expertise excuses the absence of an ingredients label. The checklist that follows is what due diligence looks like in this market — and its complexity is itself part of the argument for mandatory disclosure at the point of sale.

A practical pre-purchase checklist (each item is verifiable with free public tools — see Section 13):

C1 — Check who controls the contract. Read the contract on a block explorer. Is there a `setBaseURI` (or similar) function? Has ownership been renounced (owner set to the zero address)? If not, assume the artist/platform can change the artwork.

C2 — Check where the art is actually stored. Read the `tokenURI`; follow it to the metadata; follow the image/animation link. An `https://...company.com/...` link is a private server (fragile). An `ipfs://<hash>` link is content-addressed (better). A single company's `gateway.../ipfs/<hash>` URL is a hidden centralisation risk.

C3 — Check for an integrity hash. Look for a populated `image_hash` (or equivalent). `"none"`, blank, or absent means you cannot prove the file has not been swapped.

C4 — If it is on IPFS, secure it yourself. Pin the content to your own node or a paid pinning service, and record the native content address independently of any platform. This is the single most effective self-protection available to a consumer.

C5 — Prefer self-custody. Hold the token in a wallet you control rather than leaving it in a platform account; a platform balance is a revocable database entry.

C6 — Keep independent access. Know how to point your wallet at an alternative RPC provider or your own node, and keep your own copy of the media file. None of this makes the asset infrastructure-independent, but it removes the most common single points of failure.

C7 — Read ownership as a spectrum, not a binary. The strongest position is: fully on-chain or Arweave/IPFS-pinned art, renounced contract, populated integrity hash, self-custody. The weakest — and most common — is: private-server art, live `setBaseURI`, no hash, platform custody. Price and trust accordingly, and treat anything in the weak column as a subscription you have prepaid, not an object you own.

---

12. Conclusion

The promise of blockchain-guaranteed ownership holds for the token. It does not hold for the art.

This paper has worked through the four levels at which the promise breaks. The smart contract the buyer never controls. The file that sits on someone else's server, under someone else's domain, paid for by someone else's invoice. The gateways that mediate access to the supposedly open ledger. And underneath all of that, the basic fact that a digital artwork is not an object — it is a pattern of data that cannot be experienced without power, a device, and functioning infrastructure that no seller can guarantee and no buyer owns.

Any one of those failures, standing alone, would be enough to mean that what was sold as ownership is not ownership in any sense the law recognises. Together, they reveal something harder to ignore: this is not an edge case, not a badly designed platform, not a problem that diligent buyers

could avoid with more research. It is what the technology does by default. The seven platforms catalogued in Section 8 did not fail because they were dishonest. They failed because platforms fail — and the structure of the NFT market meant that when they did, the artwork went with them.

The "you can always download the image" defence does not survive contact with what the paper has shown. If the token certifies the image, it must be cryptographically bound to a specific file — and in the overwhelming majority of cases it is not, because the `image_hash` field that would create that binding sits empty or set to the word "none." Without that binding, the token cannot distinguish the buyer's downloaded copy from any other copy. It becomes a receipt for a transaction, not a claim to a uniquely identifiable artwork. The blockchain recorded that money changed hands. It did not record what, exactly, was sold.

The consequence for consumer protection is clear. An NFT carries the full financial commitment of an outright purchase — often a very large one, paid entirely up front — while functioning as a subscription service whose continued existence depends on the provider's goodwill, solvency, and technical choices. Subscription services are regulated as such. They disclose their terms. They are required to say what the consumer is actually paying for. NFTs are not. The least-protected position in this market is held by the consumer who paid the most.

This is not a problem that awaits new technology to solve it. It is a problem that awaits honest regulation. The recommendations in Section 11 offer a path that does not require blocking the technology, nor special expertise from buyers: a disclosure label, truthful marketing, and treatment of dependency-bearing NFT transactions as the services they are. Three principles, common to every developed legal system. The evidence in this paper is independently reproducible. The regulatory gap is demonstrable and documented. What remains is the decision to close it.

---

13. Methodology and Independent Verification

All technical findings are reproducible by any third party with free public tools.

- **Contract control:** open the contract on a block explorer (e.g., `https://etherscan.io/token/<contract>`), read the verified source for `setBaseURI`/owner functions, and call `owner()` to check for renunciation (the zero address `0x0000...0000`).
- **Storage location:** call `tokenURI(<id>)` via any public RPC endpoint, fetch the metadata, and follow the media link; inspect whether it is a private domain, an `ipfs://` content address, or a company gateway URL.
- **Integrity and tampering:** read the metadata's hash field; issue an HTTP `HEAD`/`GET` to the media URL and inspect the `Last-Modified` header and hosting headers.
- **Custody and holdings:** inspect on-chain transfer history (ERC-721 `Transfer` events, topic `0xddf252ad1be2c89b69c2b068fc378daa952ba7f163c4a11628f55a4df523b3ef`) and, for custodial platforms, the platform's public API responses.
- **Platform facts:** check the platform's public notices and announcements for shutdown dates and hosting statements.

• **RPC access restrictions:** see Infura's published compliance statements at infura.io for the documented instance of access restriction from OFAC-sanctioned regions (2022).

The observations in Section 4 regarding the Beeple Spring Collection are drawn from these same public sources and are reproducible by any third party: the contract address `0xdd012153e008346591153fFf28B0DD6724f0C256` can be inspected on Etherscan; `tokenURI` can be called via any public RPC endpoint; and Nifty Gateway's public announcements regarding its closure are available on the platform's own website and through public press records.

---

14. Glossary

• **NFT (non-fungible token):** A unique on-chain token, typically ERC-721, often used to represent ownership claims over digital art.

• **Minting:** The act of creating an NFT — deploying a smart contract and recording a new token on the blockchain. The person who mints a token controls the contract at the point of creation and sets the metadata, including any claimed artist name and artwork description. The blockchain records the minting transaction but does not verify that the minter had the right to create what they created.

• **Smart contract:** A programme stored and executed on the blockchain. In the NFT context, the smart contract manages token ownership, transfer records, and the `tokenURI` function that points to the artwork's metadata. The contract's owner — typically the artist or platform — retains administrative powers unless those powers are explicitly renounced.

• **Seed phrase / private key:** A wallet's private key is the cryptographic secret that proves control of a blockchain address and authorises transactions. The seed phrase — a sequence of twelve or twenty-four words — is the human-readable form of that secret, used to back up and restore wallet access. If the seed phrase is lost, wallet access is permanently and irrecoverably gone; no institution, court, or technical service can restore it.

• **Fungible token (e.g. ETH, BTC):** An interchangeable on-chain unit whose value is intrinsic to the token itself; unlike an art NFT, it has no separate "underlying" asset.

• **ERC-721:** The Ethereum standard defining the minimum interface for non-fungible tokens, including the `tokenURI` function.

• **EIP-2981 (NFT Royalty Standard):** An Ethereum Improvement Proposal that defines a standardised on-chain interface by which NFT contracts can signal a royalty payment obligation to marketplaces — specifying a recipient address and a royalty percentage of the sale price. EIP-2981 is a signalling standard only: it does not enforce payment. Secondary marketplaces are not technically required to honour it, and since 2022–2023, the dominant marketplaces have moved to optional or zero-royalty models that bypass EIP-2981 obligations entirely. As discussed in P3, any storage funding model that depends on secondary royalty routing must supplement EIP-2981 signalling with contract-level transfer restrictions to achieve enforceable compliance.

• `tokenURI` **/ base URI:** The on-chain pointer to a token's metadata; the base URI is the changeable component from which `tokenURI` is built.

• `setBaseURI`**:** An owner-restricted contract function that changes the base URI and redirects every token's metadata at once.

• **Metadata:** A file (usually JSON) describing the token — its name, description, and link to its image or video.

• **Contract owner / renunciation:** The account with administrative power over a contract; renunciation transfers that power to an uncontrollable address, permanently disabling owner-only functions.

• **IPFS:** A decentralised, content-addressed storage network; files are referenced by a hash of their content.

• **Pinning:** A node retaining and serving a file on IPFS; without it, content can become unreachable.

• **Arweave:** A storage network designed for permanent, paid-once data retention. Storage is funded by a one-time endowment whose yield algorithmically covers perpetual hosting costs; no ongoing payment is required after the initial deposit.

• **Filecoin:** A decentralised storage network built on top of IPFS in which storage providers make cryptographically verifiable on-chain commitments to store specific data for defined periods. Unlike passive IPFS pinning, a Filecoin storage deal is auditable on-chain, providing a programmatically verifiable proof that a specific file is being actively maintained.

• **IPFS garbage collection:** The automated storage recycling protocol by which IPFS nodes periodically evict unpinned content from their local caches to reclaim disk space. A file with no active pinner may be deleted from all nodes through this process, rendering the content address unresolvable on the network while remaining structurally valid on-chain.

• **Creative Commons Zero (CC0):** A public domain dedication under which a creator waives or relinquishes their copyrights and related rights to the maximum extent permitted by applicable law. In common law jurisdictions this typically achieves full waiver; in civil law jurisdictions (including Germany and France) where moral rights are inalienable and cannot be contractually surrendered, CC0 operates as a non-exclusive, royalty-free licence of maximum breadth rather than an absolute waiver. In the NFT context, CC0 collections eliminate the legal vacuum of a downloaded copy in most jurisdictions but simultaneously eliminate the exclusivity that justified premium pricing.

• `delegatecall`**:** A low-level Ethereum operation that allows a contract to execute code from another contract address in its own storage context. Used in proxy upgrade patterns, `delegatecall` can silently modify contract behaviour post-deployment and may not be detectable by static analysis tools examining the original contract's bytecode alone.

• **Mempool (memory pool):** The queue of pending transactions that have been broadcast to the blockchain network but have not yet been included in a confirmed block. Transactions in the mempool are publicly visible to all network participants, including automated bots that monitor it for profitable opportunities. This public visibility is the precondition for asymmetric front-running attacks.

• **Asymmetric front-running (sandwich attack):** A blockchain exploit in which an attacker monitors the public mempool, identifies a pending high-value transaction, and broadcasts a competing transaction with a higher gas fee to ensure it is mined first. In the NFT context, an attacker can observe a consumer's pending purchase and insert a `setBaseURI` mutation ahead of it in the same block, so that the consumer's purchase settles on an already-mutated asset.

Private RPC relayers eliminate this attack vector by keeping the consumer's transaction intent off the public mempool.

• **Private RPC relayer (Flashbots Protect / MEV-share):** Infrastructure services that allow users to submit transactions directly to block builders without exposing them to the public mempool. Flashbots Protect and MEV-share are the leading implementations on Ethereum. By bypassing the public mempool, these services prevent asymmetric front-running attacks, though they do not protect against state mutations committed to the chain before the consumer's transaction was submitted.

• **Static analysis tools (Slither / Mythril):** Software frameworks that analyse smart contract source code or compiled bytecode without executing the contract, identifying common vulnerability patterns, administrative function signatures, and structural risks. Slither (developed by Trail of Bits) and Mythril (developed by ConsenSys) are the leading open-source tools in this category. As discussed in R7, static analysis cannot detect all conditional execution branches that depend on runtime state, making it a necessary but not sufficient component of a compliance scanning framework.

• **RPC provider / gateway:** A commercial service through which wallets and applications read from and write to the blockchain.

• **Infura:** A leading Ethereum RPC provider operated by ConsenSys; used as the default gateway in MetaMask and many other consumer-facing applications.

• **MetaMask:** The most widely used consumer Ethereum wallet; routes blockchain traffic through Infura by default.

• **Custodial model:** An arrangement in which the platform holds tokens on the user's behalf, recording holdings in its own internal ledger rather than in the user's on-chain wallet.

• **Omnibus wallet:** A single custodial wallet holding assets belonging to many users collectively.

• **Integrity hash (`image_hash`):** A cryptographic fingerprint of the media file that allows tampering to be detected; ineffective when set to a placeholder such as `"none"`.

• **Wallet address:** A pseudonymous identifier — a string of characters derived mathematically from a private key — that represents a participant on the blockchain. A wallet address has no inherent connection to any real-world identity; the blockchain records transactions signed by the corresponding private key but cannot verify who controls that key.

---

16. Appendix A: Regulatory Alignment Notes

This appendix maps the paper's seven recommendations against existing and proposed regulatory frameworks in the two jurisdictions where formal NFT consumer-protection frameworks are most advanced: the European Union and the United States. It is provided as a practitioner reference and does not alter the jurisdiction-neutral analysis in the main body of the paper.

A.1 European Union — Markets in Crypto-Assets Regulation (MiCA)

MiCA (Regulation (EU) 2023/1114), which entered full application in December 2024, establishes a comprehensive framework for crypto-asset service providers (CASPs) operating in the EU. Several of its provisions align directly with this paper's recommendations, though significant gaps remain.

Where MiCA already provides alignment:

MiCA requires CASPs to provide clear, fair, and non-misleading marketing communications (Article 7) and to publish a crypto-asset white paper containing detailed disclosures about the asset, the issuer, and associated risks (Articles 5–6). These requirements have direct overlap with R1 (Ownership Label) and R2 (truth-in-advertising restrictions): a compliant MiCA white paper for an art NFT collection should disclose storage architecture, mutability, and custody model. However, MiCA's white paper requirements were drafted primarily with fungible crypto-assets in mind, and guidance on the specific technical disclosures this paper recommends for art NFTs does not yet exist in MiCA implementing regulations.

MiCA's custody rules (Title V) require CASPs holding client assets to segregate those assets from their own, maintain adequate records, and implement business continuity arrangements. These requirements directly support R5 (custodial transparency and segregation) and address the insolvency gap identified in Section 10.1. Platforms holding NFTs on behalf of EU consumers as a CASP are already required to segregate customer assets under MiCA.

Where gaps remain:

MiCA Article 2(3) explicitly exempts unique, non-fungible crypto-assets that are not part of a large series from core MiCA obligations — a carve-out designed for art NFTs. The practical boundary of this exemption is contested and unresolved: collections of limited edition NFTs (such as the Beeple Spring Collection's 511 tokens) may fall on either side depending on the European Securities and Markets Authority's (ESMA) forthcoming guidance. Until that guidance is issued, most art NFT issuers may lawfully claim the exemption and avoid MiCA's disclosure obligations entirely. This paper's recommendations R1 through R7 provide the substantive content that ESMA's guidance on the NFT carve-out boundary should incorporate.

MiCA does not currently address the technical specifics of storage architecture, contract mutability, integrity hashing, or compliance scanning — the subject of R4, R7, and the P-series platform recommendations. These represent a forward implementation layer that MiCA's technical standards bodies (ESMA and the European Banking Authority) should develop in their delegated acts.

Recommended action for EU practitioners: Frame R1–R3 as supplements to MiCA white paper disclosure requirements for collections that fall outside the Article 2(3) exemption, and as the basis for ESMA guidance on what the exemption's boundary should require of issuers that claim it.

A.2 United States — FTC Consumer Protection Framework

The United States does not have a comprehensive federal crypto-asset regulatory framework equivalent to MiCA. The regulatory landscape is fragmented across the Securities and Exchange Commission (securities fraud and unregistered offerings), the Commodity Futures Trading Commission (commodity derivatives), the Financial Crimes Enforcement Network (anti-money-laundering), and state-level consumer protection law. For consumer protection specifically, the primary federal instrument is Section 5 of the Federal Trade Commission Act, which

prohibits unfair or deceptive acts or practices in or affecting commerce.

Where existing US law provides alignment:

Section 5 of the FTC Act is broad enough to reach the structural misrepresentation this paper identifies. A platform that markets an NFT as providing permanent, immutable ownership — while the underlying asset sits on a mutable private server under an unrenounced contract — is making a representation about the nature and durability of the product that is materially false. The FTC's 2022 policy statement on digital deception and its enforcement history in the subscription and continuity-plan context (where sellers misrepresented the nature of recurring charges) provide direct precedent for applying Section 5 to the purchase-sold-as-subscription mischaracterisation in R3. The FTC's Green Guides (environmental marketing claims) further demonstrate the Commission's willingness to police industry-specific vocabulary claims — the NFT industry's use of "permanent," "immutable," and "own" is analogous to unsubstantiated environmental claims.

State consumer protection statutes — including California's Consumers Legal Remedies Act, New York's General Business Law sections 349–350, and equivalents in other states — provide additional grounds for pursuing the deceptive practices identified in this paper at the state level, potentially with stronger remedies including class actions and statutory damages.

Where gaps remain:

No US federal statute currently requires an NFT seller to disclose storage architecture, contract mutability, custody model, or technical attestation at the point of sale — the substance of R1, R4, R5, and R7. These disclosures could be mandated by FTC rulemaking under its Section 18 authority to issue trade regulation rules, but no such rulemaking has been initiated for NFTs specifically. The SEC's intermittent enforcement actions against NFT issuers (primarily on the basis that certain NFTs constitute unregistered securities) have not addressed the consumer-protection gap identified in this paper, and the SEC's jurisdiction does not extend to non-securities consumer goods.

The R3 non-displacement note (Section 11.1) is particularly relevant in the US context: classifying an NFT as a prepaid subscription service for consumer-protection purposes under the FTC framework is analytically independent of whether the same NFT constitutes a security under the Howey test. The FTC and the SEC have parallel but non-overlapping jurisdiction over different aspects of the same transaction.

Recommended action for US practitioners: Frame R1 and R2 as the basis for FTC rulemaking under Section 18, analogous to the FTC's existing rules on negative option marketing (16 C.F.R. Part 425) and pre-sale availability (16 C.F.R. Part 239). Frame R3 as an extension of existing FTC subscription-plan enforcement principles to the NFT context. Pursue R5 insolvency segregation requirements through state-level digital asset custody legislation, several versions of which are already in progress in New York, Wyoming, and California.

A.3 General Observation

Neither MiCA nor US federal consumer protection law currently provides the complete framework this paper recommends. MiCA is architecturally closer — its CASP framework, white paper requirements, and custody rules address several of the paper's recommendations — but its NFT exemption creates a gap precisely where the consumer harm is greatest. US law provides broad but general tools that have not been applied to the NFT-specific failures this paper documents. In both jurisdictions, the most immediate regulatory action available is the mandating of the R1 Ownership Label as a disclosure requirement, since it translates the entire technical analysis into a consumer-facing signal that existing marketing and advertising standards authorities can mandate and enforce without new primary legislation.