Crimson Publishers
Wings to the Research

Review Article

Blockchain Architecture and Software Design Focused on NFTs

Andrea Baquero[1], Danilo Torres[1], Carlos Díaz Sáenz[2], Nallig Leal[3], Fabián Ramos[3] and Esmeide Leal[3]*

[1]GIGI Group-Business Administration, Autonomous University of the Caribbean, Colombia

[2]GIIM Group-Mechatronics Engineering, Autonomous University of the Caribbean, Colombia

[3]SINT Group-Systems Engineering, Autonomous University of the Caribbean, Colombia

ISSN: 2640-9739

***Corresponding author:** Esmeide Leal, SINT Group-Systems Engineering, Calle 90 #46-112, Barranquilla, Atlántico, Colombia

Submission: April 17, 2025
Published: September 19, 2025

Volume 3 - Issue 4

How to cite this article: Andrea Baquero, Danilo Torres, Carlos Díaz Sáenz, Nallig Leal, Fabián Ramos and Esmeide Leal*. Blockchain Architecture and Software Design Focused on NFTs. COJ Elec Communicat. 3(4).COJEC.000566.2025.
DOI: 10.31031/COJEC.2025.03.000566

Copyright@ Esmeide Leal, This article is distributed under the terms of the Creative Commons Attribution 4.0 International License, which permits unrestricted use and redistribution provided that the original author and source are credited.

Abstract

Non-Fungible Tokens (NFTs) have emerged as a transformative blockchain-based technology, enabling unique digital ownership and novel applications across art, gaming and Decentralized Finance (DeFi). However, the rapid evolution of NFT ecosystems has exposed critical challenges in scalability, security and interoperability, driven by the underlying blockchain architectures and software design paradigms. This article presents a systematic review of state-of-the-art blockchain architectures supporting NFTs, analyzing Layer-1 and Layer-2 solutions, consensus mechanisms and smart contract design patterns. We further explore software design best practices for NFT platforms, including gas optimization, upgradeability and anti-fraud mechanisms. Through a comparative analysis of Ethereum, Solana, Flow and Layer-2 frameworks like Polygon, we identify trade-offs in decentralization, throughput and cost. Finally, we highlight open challenges and future directions, such as cross-chain interoperability and energy-efficient NFT minting. This work serves as a comprehensive reference for researchers and practitioners aiming to advance NFT infrastructure.

Keywords: Blockchain; NFTs; Smart contracts; Scalability; Software design; Decentralization

Introduction

The rapid evolution of blockchain technology has enabled groundbreaking innovations in digital ownership, with Non-Fungible Tokens (NFTs) emerging as a disruptive force in multiple industries. Unlike cryptocurrencies such as Bitcoin and Ethereum, which are fungible and interchangeable, NFTs represent unique assets that are verifiable on a blockchain. This distinct characteristic has fueled the adoption of NFTs in areas like digital art, gaming, music, real estate and intellectual property [1,2]. However, while NFTs have gained significant traction, the underlying blockchain infrastructure must address critical challenges related to scalability, transaction costs, security vulnerabilities and interoperability across different networks.

Scalability remains a primary concern, as high network congestion on major blockchain platforms, such as Ethereum, results in increased transaction fees and slower processing times. Layer-1 blockchains, including Ethereum, Solana and Flow, have developed unique solutions to optimize NFT transactions, yet each comes with trade-offs regarding decentralization, security and cost efficiency. Additionally, Layer-2 solutions and sidechains, such as Polygon and Immutable X, aim to alleviate these issues by offering faster, low-cost alternatives. Understanding the comparative advantages and limitations of these architectures is crucial for building efficient and sustainable NFT platforms [3,4].

Beyond blockchain scalability, software design plays a pivotal role in the functionality and user experience of NFT platforms. From smart contract development to frontend integration, software design patterns influence the security, efficiency and adaptability of NFT marketplaces [5]. Security risks such as re-entrancy attacks, metadata manipulation and phishing scams necessitate robust development strategies, including gas optimization techniques, proxy contract implementation for upgradeability and decentralized storage solutions like IPFS. Furthermore, wallet integration and indexing solutions, such as The Graph, ensure seamless user interactions and efficient metadata retrieval, enhancing the overall usability of NFT platforms [6].

As the NFT ecosystem continues to expand, research into novel blockchain architectures and software design methodologies is essential to overcome existing limitations and drive further innovation. This paper aims to provide compressive blockchain architectures and software design patterns tailored to NFT platforms [7]. By exploring the current landscape, identifying key challenges and discussing emerging technologies.

Background and Key Concepts

Blockchain technology provides the foundational infrastructure that enables the creation, transfer and verification of Non-Fungible Tokens (NFTs), ensuring decentralization, immutability and trustless verification of ownership. NFTs, as unique digital assets, are supported by a wide range of blockchain architecture, standards and smart contract ecosystems.

This section presents a technical overview of the fundamental blockchain components that underpin NFT functionality, including consensus mechanisms, token standards, smart contracts and decentralized storage. It also outlines the comparative analysis of leading NFT-compatible platforms and emerging design patterns in Decentralized Applications (dApps).

Blockchain consensus mechanism

At the core of any blockchain architecture is the consensus mechanism, which ensures agreement across distributed nodes. NFT-enabled blockchains have adopted a variety of consensus models, each influencing scalability, security and decentralization.

Proof of Work (PoW) was the initial consensus model for Ethereum, inherited from Bitcoin. PoW achieves consensus through energy-intensive computational work, offering strong security guarantees at the cost of performance and sustainability [8]. As NFT activity surged on PoW-based Ethereum, limitations such as network congestion and high gas fees became significant barriers to scalability [1].

To address these issues, Proof of Stake (PoS) emerged as a scalable and energy-efficient alternative. Networks such as Ethereum 2.0, Solana and Cardano implement PoS by requiring validators to stake tokens as collateral. This reduces the environmental impact and facilitates faster block finality, enhancing the viability of NFT marketplaces [9].

Delegated Proof of Stake (DPoS) further optimizes performance by introducing governance: token holders elect a fixed number of validators. This is implemented in platforms like EOS and Flow, where transaction throughput is prioritized without entirely compromising decentralization [10]. Each consensus model reflects trade-offs along the blockchain trilemma of decentralization, security and scalability and the choice of mechanism profoundly affects the design and performance of NFT platforms.

Smart contracts and token standards

Smart contracts autonomous programs deployed on blockchains facilitate NFT minting, ownership transfers and royalty disbursement without intermediaries. On Ethereum and EVM-compatible chains, smart contracts are written primarily in Solidity, incorporating logic for compliance with token standards. The ERC-721 standard introduced the concept of unique, indivisible tokens. Each ERC-721 token contains a unique identifier and metadata, making it ideal for representing art, collectibles and gaming assets [11]. The ERC-1155 standard extends this by allowing the management of both fungible and non-fungible tokens within a single contract, enabling batch operations and reducing gas costs a significant advancement for high-volume applications [12]. Beyond Ethereum, alternative standards have emerged: SPL tokens on Solana, FA2 on Tezos and dGoods on EOS. These standards cater to the architectural nuances of their respective chains, such as higher throughput or native support for composability and are increasingly adopted in performance-sensitive NFT applications [3]. NFTs are not just token identifiers but carriers of provenance and rights. The combination of smart contracts and token standards allows programmable logic for royalty enforcement, access control and lifecycle management, ensuring a secure and flexible asset model.

Decentralized storage and metadata integrity

While blockchains are suitable for recording ownership, storing large media files directly on-chain is impractical. Consequently, NFT metadata such as image URLs, audio or 3D models is typically stored off-chain using decentralized storage systems like IPFS (InterPlanetary File System) or Filecoin. IPFS assigns a content-addressed hash to every file, ensuring integrity and resistance to tampering [13]. However, off-chain storage introduces challenges. If a file is hosted only temporarily or through centralized gateways, the NFT risks becoming a “dead link.” To mitigate this, solutions such as Arweave offer permanent data storage models, while Metadata pinning services (e.g., Pinata) provide content persistence [14]. Maintaining this metadata integrity is essential to uphold the value and functionality of NFTs.

NFT applications across ecosystems

NFTs have redefined digital ownership and monetization across diverse industries:

Digital art: Marketplaces like OpenSea and SuperRare allow artists to mint and sell NFTs directly, embedding royalty logic into smart contracts to guarantee compensation for secondary sales [2].

Gaming: Games like Axie Infinity and Decentraland tokenize characters, land and assets, enabling cross-platform asset ownership and novel monetization models. These ecosystems leverage fast, cost-effective chains such as Ronin (for Axie) and Polygon for scalability [15].

Copyright © Esmeide Leal

DeFi integration: NFTs are used as collateral in decentralized finance platforms, enabling NFT-backed loans and fractional ownership models. Protocols like NFTfi and Arcade exemplify this convergence of DeFi and NFTs [16].

Identity and certification: NFTs are being explored for digital identity, certifications and IP protection. Academic institutions and content creators are issuing NFT-based certificates to ensure authenticity and verifiability [17].

The combination of blockchain fundamentals and NFT standards continues to evolve, addressing scalability, sustainability and interoperability challenges to foster a more efficient and inclusive digital economy.

NFT platform architectures: Categories and design context

The emergence of Non-Fungible Tokens (NFTs) as a transformative digital asset class has spurred the development of blockchain architectures specifically optimized for NFT issuance, trading and long-term asset storage. Across the rapidly evolving ecosystem, platforms differentiate themselves through variations in consensus algorithms, scalability mechanisms, transaction cost structures, developer tooling and support for composable smart contracts.

Among Layer-1 blockchains, Ethereum remains the dominant platform due to its pioneering role in defining NFT standards (ERC-721 and ERC-1155), its extensive developer ecosystem and robust support for decentralized applications. However, limitations in scalability and high gas fees have prompted the transition to Ethereum 2.0 and the growing adoption of Layer-2 solutions [18].

Other Layer-1 platforms, such as Solana and Flow, have introduced novel architectural paradigms aimed at improving performance for NFT-specific use cases. Solana's hybrid Proof-of-History (PoH) and Proof-of-Stake (PoS) consensus model enables high transaction throughput and low latency, making it attractive for applications requiring real-time interaction, despite occasional concerns about stability and decentralization [19]. Flow, developed by Dapper Labs, implements a multi-role node architecture and leverages Cadence, a resource-oriented programming language designed for digital asset management, although its unique programming model introduces a steeper learning curve [20].

To address Ethereum's scalability challenges while maintaining compatibility with its virtual machine, a growing number of Layer-2 and sidechain solutions have emerged. Polygon, for instance, aggregates technologies such as Plasma, optimistic rollups and zero-knowledge rollups, offering a versatile framework for building scalable NFT applications with lower transaction costs [12]. Similarly, Immutable X leverages zk-rollup technology to enable gas-free minting and trading of NFTs, offering an efficient and environmentally sustainable alternative for high-frequency applications such as digital collectibles and gaming [21].

In sum, the selection of a blockchain platform for NFT development must balance trade-offs between scalability, decentralization, security and ecosystem maturity. The following sections provide a deeper analysis of Layer-1 and Layer-2 solutions, as well as interoperability and alternative architectures, to inform platform selection for NFT-focused software systems.

Blockchain Architectures for NFT Applications Deployments

The design and deployment of NFT platforms are closely linked to the characteristics of the underlying blockchain architecture. As NFTs gain traction across various sectors such as digital art, gaming and decentralized finance, choosing the appropriate blockchain infrastructure becomes critical. This section provides an in-depth analysis of Layer-1 and Layer-2 solutions, alongside interoperability technologies, focusing on their implications for scalability, decentralization and security.

Layer-1 blockchains for NFTs

Layer-1 blockchains are foundational distributed ledger systems responsible for transaction validation and consensus. These include Ethereum, Solana and Flow each offering distinct architectural paradigms tailored to NFT use cases.

Ethereum remains the most widely adopted platform for NFTs, supported by a mature ecosystem and strong developer tools. Its standards, ERC-721 and ERC-1155, serve as foundational protocols for NFT issuance and interoperability [11]. However, Ethereum's original Proof-of-Work (PoW) consensus faced criticism for high energy consumption and limited throughput. With the transition to Ethereum 2.0 and adoption of Proof-of-Stake (PoS), improvements in scalability and sustainability have been realized [18]. Nevertheless, high gas fees and network congestion continue to affect NFT minting and trading activities, prompting the need for complementary Layer-2 solutions.

Solana introduces a hybrid consensus model combining Proof-of-History (PoH) with PoS to achieve high throughput reportedly up to 65,000 Transactions Per Second (TPS) and low latency. The Solana Program Library (SPL) facilitates NFT development, enabling seamless minting and marketplace integration. Despite its performance advantages, concerns remain regarding its decentralization and vulnerability to network outages [19].

Solana introduces a hybrid consensus model combining Proof-of-History (PoH) with PoS to achieve high throughput reportedly up to 65,000 Transactions Per Second (TPS) and low latency. The Solana Program Library (SPL) facilitates NFT development, enabling seamless minting and marketplace integration. Despite its performance advantages, concerns remain regarding its decentralization and vulnerability to network outages [19].

Flow, developed by Dapper Labs, was explicitly engineered for NFT centric applications. Its multi-node architecture decouples consensus, verification and execution functions to optimize scalability without compromising security. Cadence, its resource-oriented programming language, provides first-class support for digital ownership and composability [20]. Flow has powered successful NFT platforms such as NBA Top Shot, demonstrating its application-specific design benefits.

Copyright © Esmeide Leal

Layer-2 solutions and sidechains

To address Ethereum's scalability limitations, a suite of Layer-2 solutions and sidechains has emerged. These off-chain or semi-off-chain technologies process transactions separately from the Ethereum mainnet, significantly reducing fees and increasing throughput.

Polygon is a sidechain compatible with Ethereum that leverages technologies like Plasma and zk-rollups. It supports EVM-based smart contracts, enabling developers to port existing NFT projects with minimal friction. Polygon's adoption in NFT-heavy applications like The Sandbox and Decentraland illustrates its cost-effectiveness and usability [12]. See Table 1.

Table 1: Comparative analysis of NFT-compatible blockchain platforms.

Platform	Layer	Consensus Mechanism	TPS (Approx.)	Smart Contract Language	NFT Standards	Strengths	Challenges
Ethereum	Layer-1	PoW → PoS (Ethereum 2.0)	~15	Solidity	ERC-721, ERC-1155	Ecosystem maturity, composability, decentralization	High gas fees, limited throughput
Solana	Layer-1	PoH + PoS	~65,000	Rust, C, C++	SPL	High speed, low cost	Centralization risk, network instability
Flow	Layer-1	BFT-style PoS + multi-role nodes	~1,000+	Cadence	Flow NFT Standard	High scalability, tailored for NFTs	New programming model, limited tool availability
Polygon	Layer-2 (Ethereum)	PoS + Plasma / rollups	~7,000	Solidity	ERC-721, ERC-1155	Low fees, Ethereum compatibility	Dependent on Ethereum for base-layer security
Immutable X	Layer-2 (Ethereum)	zk-Rollups	~9,000	Solidity (via API/SDK)	ERC-721 (custom version)	Gasless minting, fast trading, eco-friendly	Limited customization, early-stage adoption

Immutable X is a Layer-2 protocol employing zk-rollups for gas-free NFT transactions. Built specifically for NFTs, it enables scalable, environmentally sustainable trading while inheriting Ethereum's security guarantees. Its API-first design simplifies integration for marketplaces and games [21].

Arbitrum, another Layer-2 rollup solution, focuses on general-purpose smart contract scalability with EVM compatibility. While not designed exclusively for NFTs, its low-cost transaction processing offers a viable alternative for NFT applications requiring smart contract complexity.

The trade-offs between Layer-1 and Layer-2 solutions typically revolve around the blockchain trilemma: scalability, security and decentralization. Layer-2s optimize for scalability but may introduce additional complexity in state verification and user onboarding.

Interoperability solutions

As NFT ecosystems expand across multiple blockchains, interoperability has become a pivotal concern. Achieving seamless cross-chain interactions is essential for asset liquidity, composability and user accessibility.

Cross-chain bridges such as Polkadot and Cosmos aim to connect disparate blockchains through shared security models and interoperability protocols. Polkadot employs a relay chain and parachains architecture, allowing for cross-chain messaging and asset transfers. Cosmos uses the Inter-Blockchain Communication (IBC) protocol to enable token movement between heterogeneous chains.

Wrapped NFTs represent assets from one chain to another by locking the original asset in a smart contract and issuing a synthetic counterpart. While this facilitates cross-chain access, it introduces custodial and security risks.

Standards like ERC-721 and ERC-1155 are increasingly being extended or mirrored on other blockchains (e.g., Solana's Metaplex or Tezos' FA2), fostering partial interoperability at the protocol level. Further innovations such as cross-chain messaging protocols and zero-knowledge proofs are being explored to ensure trustless verification of ownership across networks [22].

In conclusion, selecting blockchain architecture for NFT deployment requires a nuanced understanding of trade-offs in scalability, decentralization and interoperability. Layer-1 platforms offer robust security and composability, while Layer-2 solutions address cost and speed. Interoperability remains an evolving frontier, crucial for the maturation of a multichain NFT ecosystem.

Alternative architectures

Beyond traditional blockchain structures, alternative architectures are emerging to address the limitations of conventional Layer-1 and Layer-2 platforms. One such architecture is the Directed Acyclic Graph (DAG), as exemplified by Hedera Hashgraph.

DAG-based systems replace linear blockchains with a graph of transactions that can be processed in parallel, enabling high throughput and low latency. Hedera Hashgraph, in particular, utilizes a virtual voting and gossip protocol to achieve consensus, making it capable of handling thousands of transactions per second

Copyright © Esmeide Leal

with minimal energy consumption. This efficiency and deterministic finality make DAG-based systems promising for NFT applications that demand high-frequency trading and microtransactions.

Another alternative is represented by hybrid architectures like Polkadot, which combines features of both Layer-1 and Layer-2 paradigms. Polkadot introduces the concept of parachains independent blockchains that operate in parallel and communicate through a central relay chain.

This architecture allows for custom optimization of each parachain based on its intended use case, such as NFT minting, trading or metadata storage. The relay chain provides shared security and interoperability, ensuring that NFT assets can move seamlessly across parachains while maintaining trust. This modularity offers a scalable solution that balances specialization with a cohesive ecosystem.

These alternative architectures highlight a broader trend toward modular and scalable infrastructure in the NFT ecosystem. While adoption is still emerging, these models present new opportunities to resolve persistent issues of congestion, cost, and interoperability. As NFT use cases expand beyond digital art into more complex domains such as identity management and decentralized finance, these architectures may provide the necessary technological foundation for next generation NFT platforms.

In Table 2. Summarize and compare leading blockchain platforms and architectural approaches for NFT deployment, focusing on scalability, interoperability and security. The table below categorizes technologies into Layer-1, Layer-2, interoperability-focused and alternative architectures."

Table 2: Summary of blockchain architectures for NFTs.

Architecture Type	Platform / Model	Key Features	Benefits	Drawbacks
Layer-1	Ethereum	EVM-based, supports ERC-721 & ERC-1155, high decentralization	Large developer ecosystem, composability	Scalability issues, high fees
Layer-1	Solana	High throughput (400ms blocks), PoH + PoS consensus, SPL token standard	Low fees, fast transactions	Network outages, centralization concerns
Layer-1	Flow	Multi-node architecture (separates consensus and execution)	Designed for NFTs, scalable without rollups	Less decentralized than Ethereum
Layer-2 / Sidechain	Polygon	PoS sidechain to Ethereum, EVM-compatible, low gas costs	Scalability, Ethereum compatibility	Lower security than Ethereum Layer-1
Layer-2 / Sidechain	Immutable X	ZK-rollups, NFT-focused trading platform	Gasless minting/trading, Ethereum security	Centralized operator model
Layer-2 / Sidechain	Arbitrum	Optimistic rollup on Ethereum	High throughput, smart contract compatibility	Delay in finality due to fraud-proof windows
Interoperability	Polkadot	Parachain model, shared security, XCMP messaging	Scalable, parallel processing, flexible governance	Complex architecture, learning curve
Interoperability	Cosmos	IBC protocol for chain communication	Modular, high interoperability	Fragmentation risk, security varies by chain
Interoperability	Wrapped NFTs	Tokenized representations for cross-chain transfers	Enables NFT movement across chains	Increased complexity, custody risks
Alternative	Hedera Hashgraph (DAG)	Gossip-about-gossip, asynchronous Byzantine Fault Tolerance (aBFT)	High throughput, energy efficiency, fairness in ordering	Permissioned governance (Council-led)
Alternative	Hybrid (e.g., Polkadot)	Combines centralized coordination with decentralized execution	Balances of scalability and security	Trade-offs in decentralization and trust

Software Design Patterns in NFT Platforms

The development of Non-Fungible Token (NFT) platforms requires a sophisticated understanding of blockchain architecture, coupled with the implementation of efficient software design patterns. In this section, we delve into the critical aspects of smart contract design, backend and frontend considerations, and essential security mechanisms that ensure the functionality, scalability and safety of NFT ecosystems.

Smart contract design for NFTs

Smart contracts are the backbone of NFT platforms, enabling decentralized ownership and interaction without the need for intermediaries. The design of these contracts demands best practices to ensure both efficiency and security. One of the key components in smart contract development is gas optimization. Gas costs are a crucial consideration on platforms like Ethereum, where each transaction requires a fee for processing. Optimizing gas usage ensures that transactions are executed more efficiently and cost-effectively. Techniques such as minimizing state changes, using mappings instead of arrays and utilizing efficient algorithms for storage access are standard practices for reducing gas consumption.

Additionally, upgradeability is an essential design consideration for NFTs. Due to the immutable nature of blockchain, once a smart contract is deployed, it cannot be modified. However, NFT platforms often require updates and improvements to stay competitive. The Proxy Pattern allows for smart contracts to be updated by routing

 Copyright © Esmeide Leal

transactions to a separate, upgradable contract, ensuring that the core contract logic remains upgradeable without losing data (Liu & Wang, 2020). The Diamond Standard is another approach for handling upgradeability. This pattern allows for multiple contract facets to be upgraded independently, offering a more flexible solution to contract management. Ensuring that these contracts are secure is paramount. Common vulnerabilities like reentrancy attacks, where malicious actors exploit a contract's call function to steal funds and overflow errors, which can lead to unintended behaviors, must be mitigated through rigorous validation and checks during development.

Backend and frontend considerations

Beyond smart contract development, the backend and frontend architecture of NFT platforms must also be designed with scalability and usability in mind. On the backend, indexing solutions like The Graph provide a powerful tool for querying blockchain data in a decentralized way. The Graph allows for efficient retrieval of NFT metadata, transactions and other critical information, enabling the development of fast and responsive dApps. By indexing blockchain data, developers can avoid the need to directly query the blockchain every time a user interacts with an NFT, reducing delays and improving the overall performance of platform [23].

Wallet integration is another critical aspect of NFT platforms. Wallets like MetaMask and Wallet Connect provide users with a way to interact securely with the blockchain without exposing their private keys. These tools enable users to connect their cryptocurrency wallets to NFT platforms, facilitating seamless transactions.

MetaMask, as one of the most widely adopted Ethereum-based wallets, is often the go-to solution for users engaging with NFT marketplaces. By supporting standard interfaces like Web3.js, these wallets help developers create a smooth interaction between the frontend and the blockchain [24]. As NFT platforms grow in popularity, ensuring seamless wallet integration becomes crucial for user adoption and experience

Security and anti-fraud mechanisms

Security is an overarching concern in the development of NFT platforms, particularly due to the irreversible and immutable nature of blockchain transactions. The decentralized nature of these platforms means that once assets are transferred, they cannot be retrieved unless the platform implements strong anti-fraud measures. One common vulnerability is reentrancy attacks, which can occur when an attacker exploits a vulnerability in the contract to perform unauthorized actions, such as withdrawing funds multiple times. Preventative measures include the use of checks-effects-interactions patterns and ensuring that external calls are minimized in the contract code [17].

Phishing is another significant threat, as users may be tricked into revealing their private keys or approving malicious transactions. To combat this, NFT platforms must adopt anti-phishing mechanisms, such as alerting users to suspicious URLs or offering educational content on identifying fraudulent activity. These mechanisms can be enhanced through collaboration with cybersecurity experts to create robust user verification systems.

Finally, oracles are integral to the functioning of dynamic NFTs, which are NFTs whose attributes change over time based on real-world data or events. Oracles provide external data to smart contracts, allowing them to react to real-world conditions, such as sports scores or weather changes. However, ensuring the reliability and security of oracles is critical, as unreliable data could lead to inconsistencies or malicious manipulation of dynamic NFTs. To mitigate these risks, it is essential to utilize trusted oracle services that offer multiple data sources and decentralized verification [25].

Multilevel Tests for Blockchain Architecture Applied in NFT

A project of this type implements a comprehensive testing strategy that covers multiple levels, with special emphasis on the security and reliability required for Blockchain platforms. It consists of the following items [26]:

Component-based testing approach

Smart contracts (high criticality):

A. Exhaustive unit tests for minting and transfer contracts with a minimum coverage of 95%.

B. Verification of correct ownership assignment and metadata management.

C. Validation of transfer and royalty distribution functions.

D. Specialized audit for vulnerability detection.

E. Tools: Truffle, MythX [27].

Backend (high criticality):

a) Integration tests for authentication and user management services.

b) Validation of endpoints for registration, login, and session management.

c) Verification of integrity in IPFS metadata storage and retrieval.

d) Tools: Jest, Mocha, Chai, Postman.

Frontend web and mobile (medium-high criticality):

A. E2E tests for critical flows such as NFT purchasing.

B. Validation of collection display and rendering.

C. Responsive design and resource optimization testing.

D. Tools: Cypress, Flutter Test [28].

Types of tests implemented

a) Unit Tests: Verification of isolated components, triggered on each commit.

b) Integration Tests: Validation of interaction between components using Cypress and Postman [29,30].

Copyright © Esmeide Leal

c) E2E Tests: Simulation of complete user flows, triggered upon promotion to staging.

d) Contract Tests: Specific verification of smart contracts in simulated environments.

e) Performance Tests: Analysis of behavior under load using JMeter, scheduled weekly.

f) Static Analysis: Verification of coding standards and vulnerability detection using ESLint.

g) Security Tests: Threat detection using OWASP ZAP and specific audits for Blockchain.

Established coverage levels

The coverage levels established within the framework of a Component Testing Approach refer to the different metrics used to measure the comprehensiveness of the tests carried out at the level of individual components of a software. The main purpose of these levels is to determine which parts of the component code have been exercised by testing and therefore identify areas that might not have been adequately tested [31,32]. The following are suggested data (Table 3):

Table 3: Coverage levels established within the framework of a component testing approach.

Component	Minimum Coverage	Justification
Smart Contracts	95%	Handle valuable digital assets
Authentication Services	90%	Critical for access security
Transaction APIs	90%	Essential for financial operations
Critical UI Components	85%	Related to transactions
Secondary UI Components	70%	Non-critical informational elements
Mobile Application - Critical Modules	90%	Transaction functionalities
Mobile Application - Secondary Modules	75%	Navigation and informational components

User experience testing

This should consider the following:

A. Usability evaluation with representative user groups (artists and buyers).

B. Analysis of critical interfaces such as wallet connection and minting processes.

C. Validation of clarity in transaction signing requests.

D. Experience testing under intermittent connection conditions for the mobile app.

The testing strategy must be fully integrated with the development process through an automated CI/CD pipeline, ensuring early detection of issues and maintaining high quality standards, particularly important in a system handling valuable digital assets in a blockchain environment.

Open Challenges and Future Directions

Scalability

Definition: Scalability addresses the ability of the underlying blockchain network to handle a large volume of NFT transactions (minting, trading, transferring) quickly and affordably [33,34].

Challenge: Many popular blockchains (historically Ethereum) face congestion when NFT activity surges. This leads to slow transaction confirmation times and extremely high transaction fees (often called “gas fees”), making NFTs expensive and frustrating to use, especially for lower-value items or high-frequency actions.

Future direction/solutions (sharding & rollups):

A. Sharding: This is a database partitioning technique applied to blockchains. It involves splitting the network’s data and transaction processing load across multiple smaller, parallel chains (“shards”). The idea is that by processing transactions concurrently on different shards, the overall capacity (throughput) of the network increases significantly, reducing congestion and fees. Ethereum is implementing forms of sharding as part of its ongoing upgrades.

B. Rollups (Layer 2 scaling): These are solutions built “on top” of the main blockchain (Layer 1). They bundle or “roll up” hundreds of transactions off-chain, process them efficiently and then post a compressed summary or proof back to the main chain. This drastically reduces the data load and computational burden on Layer 1, leading to much lower fees and faster transaction speeds for users interacting with the rollup. Examples include Optimistic Rollups (like Optimism, Arbitrum) and Zero-Knowledge Rollups (like zkSync, StarkNet).

Goal: To make NFT interactions seamless, fast and cheap, regardless of network activity levels.

Interoperability

Definition: Interoperability refers to the ability of different blockchain networks to communicate and interact with each other, allowing assets like NFTs to be recognized, transferred or used across multiple chains.

Challenge: Currently, most NFTs are “siloed” on the blockchain where they were minted (e.g., an Ethereum NFT isn’t easily usable on Solana). This fragmentation limits an NFT’s utility, reach and potential value and complicates the user experience.

Copyright © Esmeide Leal

Future direction/solutions (cross-chain NFT standards & protocols):

a) **Cross-chain NFT standards:** Developing common technical standards or protocols that define how NFTs should be represented and transferred between different blockchains. This would allow wallets, marketplaces, and applications on different chains to understand and interact with the same NFT.

b) **Protocols like CCIP & wormhole:** These are examples of cross-chain messaging and interoperability protocols.

c) **CCIP (Chainlink cross-chain interoperability protocol):** Aims to provide a secure way for smart contracts on one chain to communicate, send messages, and initiate transactions (including token/NFT transfers) on another chain.

d) **Wormhole:** A generic messaging protocol that connects various high value blockchains, enabling the transfer of data and assets (including NFTs, often by "locking" the original on one chain and "minting" a representation on another) across them.

Goal: To create a seamless "internet blockchains" where NFTs can move and be utilized freely across different ecosystems, enhancing their value and user experience.

Sustainability

Definition: Sustainability in the NFT context primarily concerns the environmental impact, specifically the energy consumption, associated with the blockchain networks NFTs rely on [35].

Challenge: Early and prominent blockchains like Bitcoin and (until September 2022) Ethereum used Proof-of-Work (PoW) consensus mechanisms. PoW requires vast amounts of electricity for "mining" (validating transactions and securing the network), leading to significant carbon footprint concerns and public criticism directed at NFTs minted on these chains.

Future direction/solutions (energy-efficient consensus):

A. **Shift to Proof-of-Stake (PoS):** This is the primary solution being adopted. PoS relies on validators "staking" their own cryptocurrency as collateral to validate transactions. It does not involve energy-intensive computation like PoW. Ethereum's transition ("The Merge") to PoS dramatically reduced its energy consumption (by ~99.95%). Many newer blockchains are built on PoS or similar efficient mechanisms from the start.

B. **Other efficient mechanisms:** Exploration and use of other consensus protocols that are inherently less energy-intensive than PoW.

Goal: To ensure that the creation and trading of NFTs occur on blockchain infrastructure that is environmentally friendly and energy-efficient, addressing public concerns and aligning with broader sustainability goals.

Regulatory & legal aspects

Definition: This encompasses the evolving body of laws, regulations and legal interpretations surrounding the creation, ownership, sale and use of NFTs [36].

Challenge: NFTs are a novel technology operating in a rapidly evolving digital space. Existing legal frameworks (e.g., for property, contracts, intellectual property, securities) often don't directly or clearly apply. This creates uncertainty for creators, buyers, platforms and regulators.

Future direction/focus (intellectual property rights):

A. **Intellectual Property (IP) rights:** A key area of confusion and legal challenge. Buying an NFT typically grants ownership of the token itself on the blockchain, but not automatically the underlying copyright or other IP rights to the associated artwork, music, video or other content. The specific rights transferred (e.g., right to display, commercialize) depend entirely on the terms set by the creator, often specified in the NFT's metadata or a separate license agreement. Lack of clarity, inconsistent terms and enforceability issues are major challenges.

B. **Other areas:** Besides IP, challenges include: classifying NFTs (are they collectibles, securities, commodities?), taxation rules for NFT profits/losses, Anti-Money Laundering (AML) and Know Your Customer (KYC) compliance for marketplaces, consumer protection issues and jurisdictional complexities in cross-border transactions.

Goal: To establish clearer legal frameworks, regulations and best practices that provide certainty, protect creators and consumers, define ownership and usage rights (especially IP), and integrate NFTs responsibly into existing legal and financial systems.

These areas represent significant hurdles but also crucial opportunities for innovation that will shape the future development and mainstream acceptance of NFTs.

Conclusion

Non-Fungible Tokens (NFTs) represents a significant paradigm shift in digital ownership, leveraging blockchain technology to provide verifiable uniqueness for assets across diverse sectors like art, gaming, finance and identity. While the potential applications are vast and transformative, the rapid growth of the NFT ecosystem has brought critical infrastructural and design challenges to the forefront. This investigation highlights that the underlying blockchain architecture and the specific software design patterns employed are paramount in addressing these hurdles and realizing the full potential of NFTs. A central theme is the persistent tension between scalability, security and decentralization of the blockchain trilemma. The solutions like Ethereum, Solana and Flow offer distinct approaches, each with inherent trade-offs. Ethereum, despite its established ecosystem and robust smart contract capabilities (ERC-721, ERC-1155), has historically struggled with high gas fees and low throughput, though solutions and its transition to Proof-of-Stake aim to alleviate this.

High-performance chains like Solana offer speed and low costs but face questions regarding network stability and

Copyright © Esmeide Leal

centralization. Purpose-built platforms like Flow prioritize scalability for collectibles through unique architectures but introduce new programming paradigms. However, the rapid growth of the NFT ecosystem highlights critical challenges related to the underlying blockchain architectures and software design, primarily in scalability, security, and interoperability. Software design is equally critical, with best practices in smart contract development (including gas optimization and upgradeability patterns), backend/frontend integration (like indexing and wallet support) and robust security measures being essential for creating efficient, secure and user-friendly NFT platforms. Furthermore, rigorous, multi-level testing strategies are vital to ensure the reliability and security of these platforms, particularly given the financial value often involved. Significant open challenges remain, including achieving seamless cross-chain interoperability, enhancing scalability through techniques like sharding and rollups, ensuring environmental sustainability by adopting energy-efficient consensus mechanisms like PoS and navigating the complex and evolving regulatory and legal landscape, especially concerning intellectual property rights. Addressing these challenges is crucial for the continued development and mainstream adoption of NFTs. This document serves as a comprehensive overview of the current state, architectural considerations, design patterns and future directions for researchers and practitioners working to advance NFT infrastructure.

References

1. Wang Q, Li R, Wang Q, Chen S (2021) Non-Fungible Token (NFT): Overview, evaluation, opportunities and challenges. ArXiv: 2105.07447.
2. Regner F, Urbach N, Schweizer A (2019) NFTs in practice-non-fungible tokens as core component of a blockchain-based event ticketing application. In Proceedings of the 40th International Conference on Information Systems (ICIS).
3. Zamyatin A, Al-Bassam M, Zindros D, Kokoris-Kogias E, Moreno-Sanchez P, et al. (2021) SoK: Communication across distributed ledgers. IEEE Symposium on Security and Privacy.
4. Wood G (2014) Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper.
5. Atzei N, Bartoletti M, Cimoli T (2017) A survey of attacks on Ethereum smart contracts (SoK). In International Conference on Principles of Security and Trust, pp. 164-186.
6. Torres C, Steichen M, State R (2019) The art of the scam: Demystifying honeypots in Ethereum smart contracts. USENIX Security Symposium.
7. Ferreira A, Velasquez K (2023) Smart contract design patterns and best practices for NFT marketplaces. Journal of Web Engineering 22(4).
8. Narayanan A, Bonneau J, Felten E, Miller A, Goldfeder S (2016) Bitcoin and cryptocurrency technologies. Princeton University Press, USA.
9. Buterin V (2021) Ethereum 2.0: Proof-of-stake and beyond. Ethereum Foundation.
10. Zheng Z, Xie S, Dai H, Chen X, Wang H (2017) An overview of blockchain technology: Architecture, consensus and future trends. Proceedings of the IEEE 106(5): 104-125.
11. Entriken W, Shirley D, Evans J, Sachs N (2018) ERC-721: Non-fungible token standard. Ethereum Improvement Proposals.
12. Radomski E, Castonguay A, Saft J (2018) ERC-1155 multi token standard. Ethereum Improvement Proposal.
13. Benet J (2014) IPFS-content addressed, versioned, P2P file system. arXiv:1407.3561.
14. Ogata K, Fujita S (2023) Decentralized storage with access control and data persistence for e-book stores. Future Internet 15(12): 406.
15. Tavares R, Sousa JP, Maganinho B, Gomes JP (2023) Gamers' reaction to the use of NFT in AAA video games. Procedia Computer Science 219: 606-613.
16. Sasha S (2022) A comprehensive study on Non-Fungible Tokens (NFTs): Use cases, ecosystem, benefits & challenges.
17. Lopez LJ, Ledezma GG (2025) Employing blockchain, NFTs and digital certificates for unparalleled authenticity and data protection in source code: A systematic review. Computers 14(4): 131.
18. Buterin V (2021) A rollup-centric Ethereum roadmap. Ethereum Foundation Blog.
19. Mishra DP, Behera SR, Behera SS, Patro AR, Salkuti SR (2024) Solana blockchain technology: A review. International Journal of Informatics and Communication Technology (IJ-ICT) 13: 197.
20. Zaucha T, Agur C (2022) Newly minted: Non-fungible tokens and the commodification of fandom. New Media & Society 26(4): 2234-2255.
21. Anglen J. What is immutable X? The leading layer 2 solution for NFTs. Rapid Innovation.
22. Pillai B, Biswas K, Muthukkumarasamy V (2020) Cross-chain interoperability among blockchain-based systems using transactions. The Knowledge Engineering Review 35: e23.
23. Liu M, Wang H, Yang F (2021) An efficient data query method of blockchain based on index. 7th International Conference on Computer and Communications (ICCC).
24. Nainar A, Vigneshwaran, Surya, Kumar S, Kanna S (2023) Blockchain-based decentralized E-commerce using Ethereum and smart contracts. International Journal of Innovative Science and Research Technology 8(3):
25. Soloukia M, Bamakanb SM (2022) An in-depth insight at digital ownership through dynamic NFTs. Procedia Computer Science. 214: 875-882.
26. Destefanis G, Flynn L, Guerrero-Contreras G, Ortu M (2023) Smart contract testing: An analysis of the state of the art and future directions. ACM Computing Surveys 55(10s): 1-37.
27. Golosova A, Proper HA (2022) A systematic literature review on smart contract security analysis and testing. Computers & Security 118: 102711.
28. Wöhrer M, Zdun U (2020) A systematic literature review on the security testing of smart contracts. Blockchain: Research and Applications 1(2): 100007.
29. Lin H, Jia X, Zhang S, Wu J, Qian P, et al. (2024) NFT mark: A testing framework for NFT marketplaces. Journal of Systems and Software 209: 111961.
30. Li S, Qin B, Zhao Z (2022) A survey on blockchain testing: Concepts, challenges and future directions. Journal of Systems and Software 193: 111438.
31. Wan Z, Gao Z, Ren Y, Xu X (2021) Towards continuous integration and continuous deployment for blockchain applications: A case study of hyperledger fabric. IEEE Access 9: 111491-111503.
32. Porru S, Pinna A, Marchesi M, Tonelli R (2020) A systematic literature review on blockchain technology in the energy sector. Journal of Cleaner Production 258: 120775.
33. Nadilo T, Nadilo M, Šerić L (2023) Non-Fungible Tokens (NFT): Review of the literature and future research agenda. Journal of Risk and Financial Management 16(11): 466.

Copyright © Esmeide Leal

34. Wang Q, Li R, Wang Q, Chen S (2021) Non-Fungible Token (NFT): Overview, evaluation, opportunities and challenges. arXiv:2105.07447.

35. Ante L (2023) Non-Fungible Token (NFT) markets: A survey of the state of the art. FinTech 2(2): 116-130.

36. Guadamuz A (2021) The treachery of images: Non-fungible tokens and copyright. Journal of Intellectual Property Law & Practice 16(12): 1367-1385.

Copyright © *Esmeide Leal*