

ORGANIZED BY



Frankfurt School
Blockchain Center

Follow us on



Medium

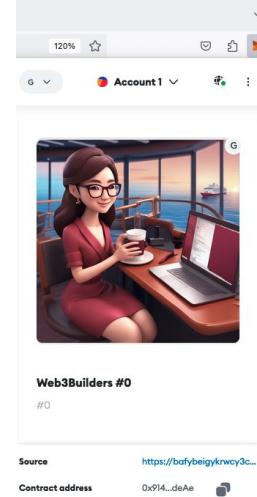


NFT Talents

Assignment 3: Technical Aspects of NFTs

August 22, 2023

Karen Yang



Partners



With donations from



Supported by



Assignment 3

The screenshot shows the Remix Ethereum IDE interface. The top bar displays the URL <https://remix.ethereum.org/#lang=en&optimize=true&runs=200&evmVersion=null&version=soljson-v0.8.18+commit.87f61d96.js> and a zoom level of 120%. The interface includes a FILE EXPLORER on the left and a code editor on the right.

FILE EXPLORER:

- WORKSPACES:
 - ERC-721 Smart Contract NFT
- contracts
 - artifacts
 - 1_Storage.sol
 - 2_Owner.sol
 - 3_Ballot.sol
- Web3Builders.sol
- scripts
- tests
- .deps
- README.txt
- .prettierrc.json

Code Editor (Solidity Contract: Web3Builders.sol):

```
51 // Add payment
52 function publicMint() public payable {    infinite gas
53     require(publicMintOpen, "Public Mint Closed");
54     // public mint price is 0.01
55     require(msg.value == 0.01 ether, "Not Enough Funds");
56     internalMint(); // call function to handle internal
57 }
58
59 function internalMint() internal {    infinite gas
60     // Add limiting supply, Total Supply keeps track of what has been minted
61     require(totalSupply() < maxSupply, "We Sold out!");
62     // keeps track of how many token ids
63     uint256 tokenId = _tokenIdCounter.current();
64     _tokenIdCounter.increment();
65     // minter is sender wallet address
66     _safeMint(msg.sender, tokenId);
67 }
68
69 }
70 // get balance of contract and transfer it to address specified
71 function withdraw(address _addr) external onlyOwner {    infinite gas
72     // get the balance of the contract
73     uint256 balance = address(this).balance;
74     payable(_addr).transfer(balance);
75 }
76
77
78 // Populate the allowList
79 function setAllowList(address[] calldata addresses) external onlyOwner {    infinite gas
80     //append addresses in array into allowList mapping, set value to true
81     for(uint256 i=0; i < addresses.length; i++){
82         allowList[addresses[i]] = true;
83     }
84 }
```

At the bottom of the code editor, there are buttons for 'listen on all transactions' and a search bar labeled 'Search with transaction hash or address'.

Assignment 3

The screenshot shows the Pinata Cloud Pin Manager interface. The left sidebar has a dark theme with icons for Pinata, Files (selected), Gateways, API Keys, Private API Keys, Access Controls, and Documentation. The main area is titled "Files" and shows two pinned files:

Name	Content Identifier (CID)	Actions
Web3Builders Metadata	QmbtYbmMb3yUee4RYVjoAN4hLCrWUJNQDGPGQvbqhK39RE	Share More
Web3Builders	Qmcu7SEv8XrtD4yILKxJpd1KtJ6JT8IQx1ZiCTpWp3JNM	Share More

At the bottom, there are navigation arrows (< 1 >) and a footer with "Slide 3 | website" and the NFT Talents logo.

Assignment 3



A screenshot of a web browser displaying an IPFS file listing. The URL in the address bar is `gateway.pinata.cloud/ipfs/Qmcu7SEv8XrtD4yiLKxJpd1KtJ6jT8iQx1ZiCTpWp3JNM/`. The page title is "IPFS". On the right, there are links for "About IPFS", "Install IPFS", and a download icon. Below the title, it says "Index of /ipfs/Qmcu7SEv8XrtD4yiLKxJpd1KtJ6jT8iQx1ZiCTpWp3JNM" and shows a file size of "1.7 MB". The file list includes four files: 0.png, 1.png, 2.png, and 3.png, each with their respective IPFS hash and file size.

File	Hash	Size
0.png	QmVJ...hgAN	444 kB
1.png	QmZM...idUG	450 kB
2.png	QmSn...iNoA	398 kB
3.png	Qme4...htbo	418 kB

Assignment 3

https://testnets.opensea.io/assets?search[query]=0x914206bd451bcDF30e1C4241496239daE7C5deAe

NEW RELEASE

Introducing Deals Now you can offer your NFTs for their NFTs. [Make a deal](#)

OpenSea Testnets

Drops Stats

Search items, collections, and accounts

0.7159 ETH | 0 WETH

Sort

Collection results



Web3Builders

0 items

0x914206bd451bcDF30e1C4241496239daE7C5deAe X

Assignment 3

Deploy & Run Transactions ✓

Transactions recorded 3 ⓘ ➡

Deployed Contracts

WEB3BUILDERS AT 0x914206bd451bcdf30e1c4241496239dae7c5deae

Balance: 0.01 ETH

allowListMint

approve address to, uint256 tokenId

editMintWindows

_publicMintOpen: true

_allowListMintOpen: true

Calldata Parameters **transact**

pause

publicMint

renounceOwn...

safeTransferFr... address from, address to, uint

Home Web3Builders.sol

108 // Contract Address: 0x914206bd451bcdf30e1c4241496239dae7c5deae
109 // https://goerli.etherscan.io/tx/0x8850976f299eefb79fffd852f59a1
110 //
111 // editMintWindow, true, true transact
112 // https://goerli.etherscan.io/tx/0xc15e7ed9a9d34e85c17c7e64a4c70
113 //
114 // PublicMint
115 // Value: 1000000 Gwei
116 // 0x914206bd451bcDF30e1C4241496239daE7C5deAe
117 // https://goerli.etherscan.io/tx/0x6c374d640a69bc74dc44136f9251cd
118 //
119 //OpenSea Testnet
120 // https://testnets.opensea.io/assets?search[query]=0x914206bd451
121 //
122

G Account 1

Tokens NFTs Activity

Unnamed c... #0

Web3Builders (1)

Import NFT Refresh list MetaMask support

0 listen on all transactions Search with transaction hash or address

status	true Transaction mined and execution succeeded
transaction hash	0x6c374d640a69bc74dc44136f9251cd8e8f6f8db69225
block hash	0x6e0f557cf6ec354b9deefe3e4f59ec57d882e1fe0b4
block number	9535030
from	0x147F347ced59C0fd5281Fc831Ad35fF2D2e1AE23
to	Web3Builders.publicMint() 0x914206bd451bcDF30e1C4241496239daE7C5deAe
gas	128986 gas



NFT Media Storage Options

**Where is NFT media actually saved?
What options are there?**

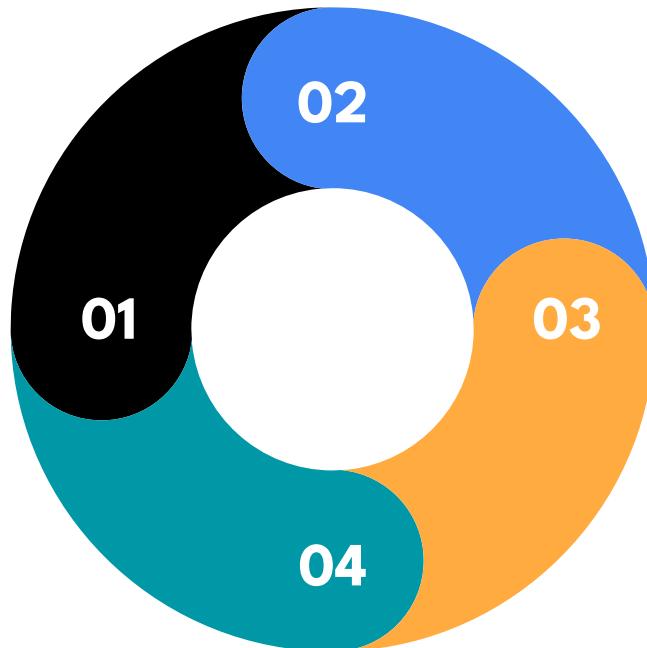
This section provides an overview of the various options available for storing NFT media.



On-Chain Storage

Some blockchains, like Ethereum, support on-chain storage of smaller files directly within the NFT smart contract.

Media is stored directly on the blockchain.



Limited file size due to blockchain constraints.

Can be expensive in terms of gas fees.

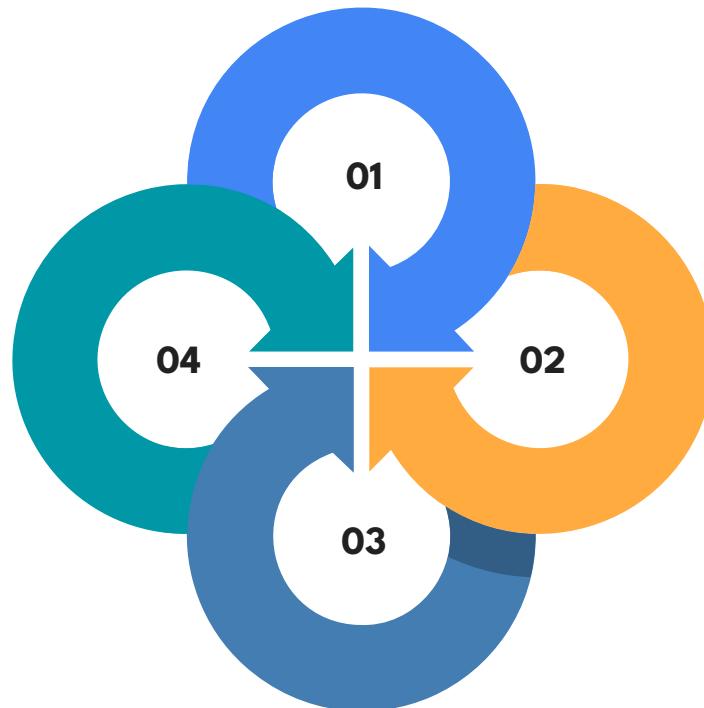
Off-Chain Storage with IPFS

Only metadata and a reference to the file are stored on the blockchain.

More efficient storage and reduces burden on the blockchain.

IPFS (InterPlanetary File System) allows for decentralized storage and sharing of files.

NFT platforms use IPFS to store media files off-chain.





Centralized Cloud Storage

- NFT platforms may use centralized cloud storage solutions like AWS or Google Cloud.
- Media files are hosted on the cloud.
- NFT token contains a link or reference to the storage location.
- Dependent on the reliability and availability of the cloud provider.



Decentralized Storage Networks

- 01** Alternative options for storing NFT media.
- 02** In addition to IPFS, decentralized storage networks like Filecoin and Swarm can be used.
- 03** Similar to IPFS, offering decentralized and distributed storage.
- 04** Can provide increased resilience and censorship resistance.

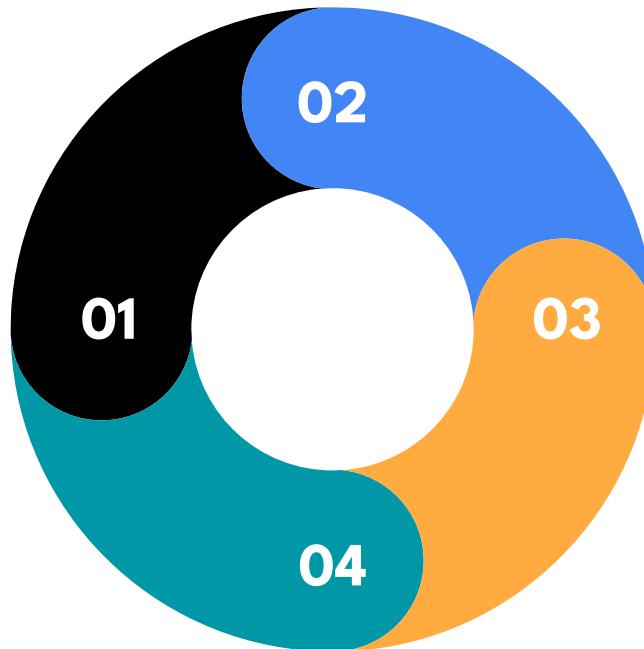
Layer 2 Solutions

Layer 2 scaling solutions, like sidechains or rollups, can store NFT media.

Operate off the main blockchain for faster and cheaper transactions.

Suitable for larger file sizes associated with NFTs.

Enhanced scalability and cost-efficiency.



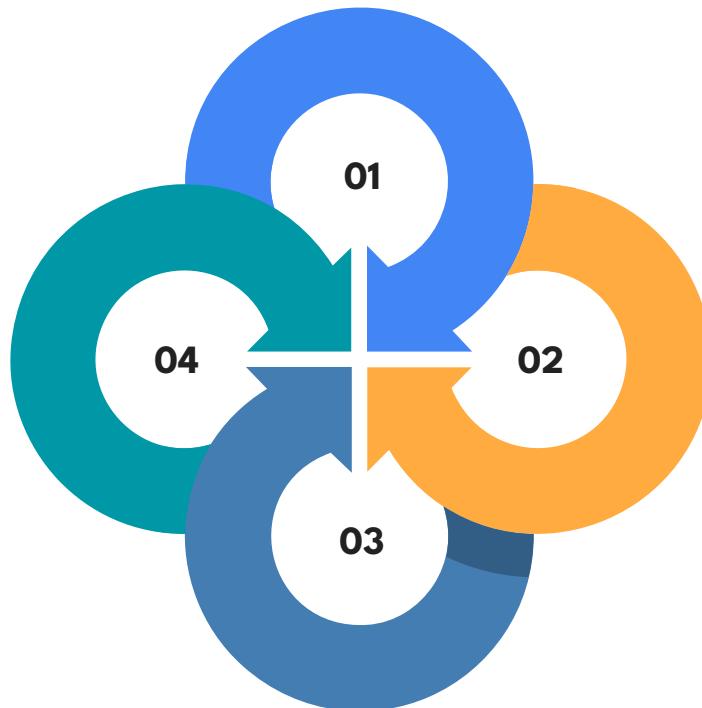
Hybrid Approaches

Optimizing storage solutions based on specific needs.

Customizable and adaptable approaches.

Some platforms use a combination of methods to balance efficiency, security, and cost.

Smaller previews stored on-chain, full-resolution media off-chain using IPFS or other decentralized storage.



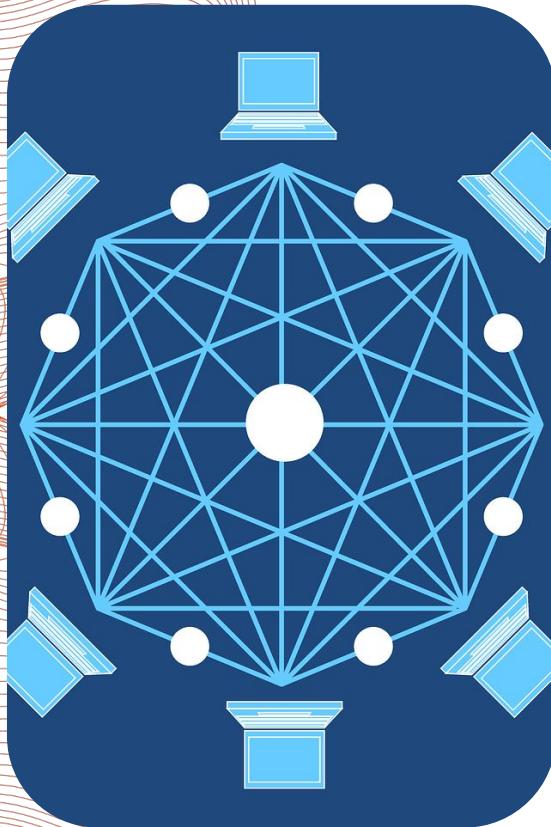


Risks Associated with Storing NFT Media

What are the risks associated with the different methods of storing NFT media?

This section explores the risks and considerations associated with different methods of storing NFT (Non-Fungible Token) media.





On-Chain Storage

01

Blockchain Bloat: Storing large files on-chain can contribute to blockchain bloat, which can impact the scalability and efficiency of the blockchain network.

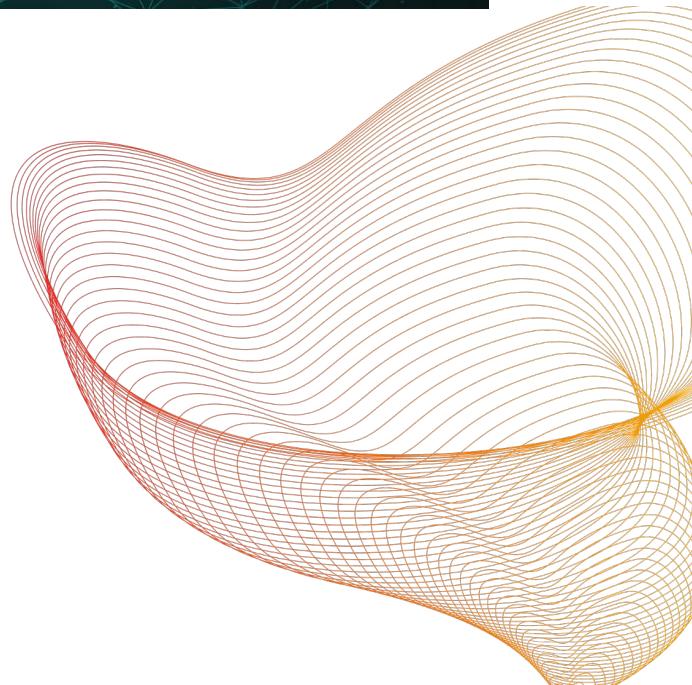
02

High Gas Fees: Storing media directly on the blockchain can lead to high gas fees, especially for larger files. This can make it expensive to create or interact with NFTs.



Off-Chain Storage with IPFS

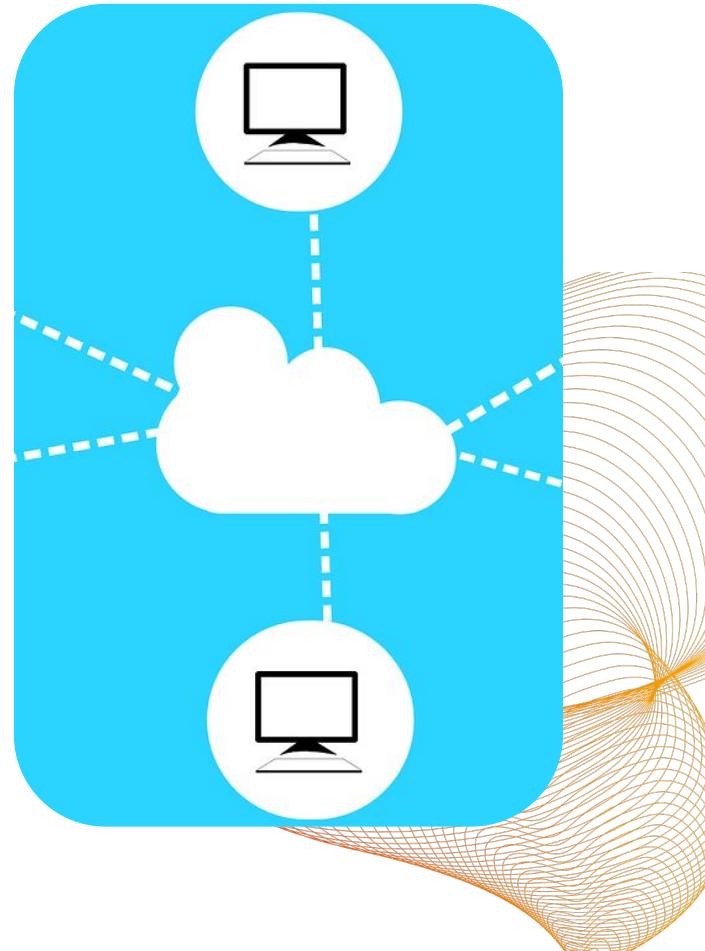
- **Content Availability:** While IPFS is designed for decentralized storage, there can still be instances where the content is not available due to network or node issues. This can result in broken links or unavailable media.
- **Longevity:** The availability of IPFS content relies on the network's participants. If there's a lack of interest or maintenance, the files might become inaccessible over time.



Centralized Cloud Storage

- 01** **Data Loss:** If the centralized storage provider experiences data loss or goes out of business, the NFT media could become permanently inaccessible.

- 02** **Centralization:** Storing NFT media on centralized servers is counter to the decentralized nature of blockchain technology and NFTs. It can expose the content to censorship and control by a single entity.





Decentralized Storage Networks (Filecoin, Swarm, etc.)

- **Complexity:** Using decentralized storage networks might introduce technical complexities for users and developers who are not familiar with these systems.
- **Token Economics:** Some decentralized storage networks use tokens to incentivize participants. Fluctuations in token value or changes in network economics can affect the accessibility and cost of storing and retrieving NFT media.





Layer 2 Solutions

- **Dependency on Main Chain:** Layer 2 solutions depend on the security of the main blockchain. If the main chain experiences a security breach or other issues, it could impact the integrity of NFT media stored on layer 2.





Hybrid Approaches

- **Coordination Complexity:** Managing hybrid storage methods might introduce additional complexities in terms of coordination between onchain and off-chain components.





NFT Risks and Security

**What risks do NFT investors need to understand?
What common methods are used to steal NFTs?**

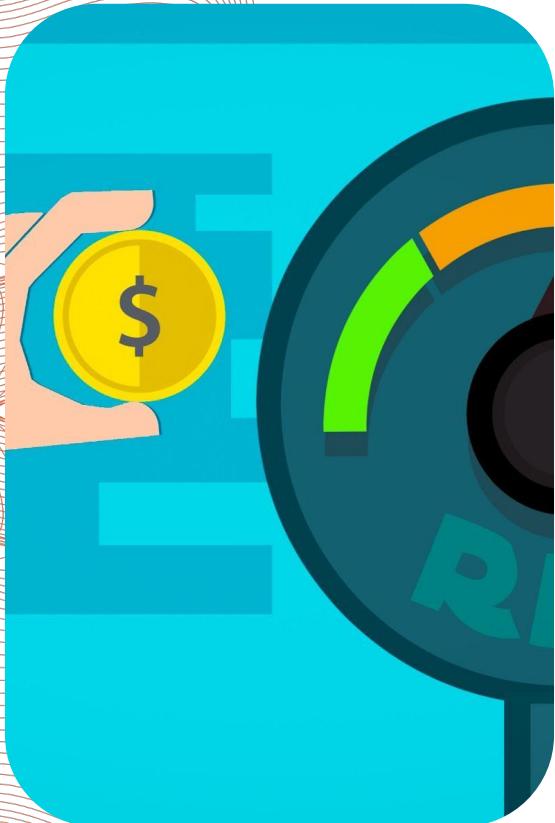
This section covers the risks associated with NFT investments and common methods used to steal NFTs, as well as strategies to mitigate risks and protect NFT holdings.





Risks of NFT Investments

- **Market Volatility:** NFTs can experience rapid and significant fluctuations in value.
- **Lack of Regulation:** The NFT market is relatively new and evolving, leading to a lack of comprehensive regulatory oversight.
- **Liquidity Issues:** Some NFTs may be difficult to sell quickly, especially during market downturns.
- **Market Sentiment:** NFT prices can be influenced by market sentiment, trends, and hype.
- **Copyright and Ownership Challenges:** Ownership of an NFT doesn't necessarily grant full copyright or intellectual property rights.
- **Tech and Platform Risks:** NFTs are built on blockchain technology, making them susceptible to technical issues, hacks, and platform changes.
- **Storage and Access Concerns:** Risks of files becoming inaccessible, lost, or corrupted over time.
- **Scams and Counterfeits:** Instances of fake NFTs being sold and scams involving misleading project promises or phishing attempts.
- **Market Saturation:** Increasing competition and potential impact on the value of individual NFTs.
- **Economic Factors:** Influence of macroeconomic trends, cryptocurrency market movements, and investor sentiment.
- **Environmental Concerns:** Some NFT platforms contribute to carbon emissions, leading to reputational and regulatory risks.



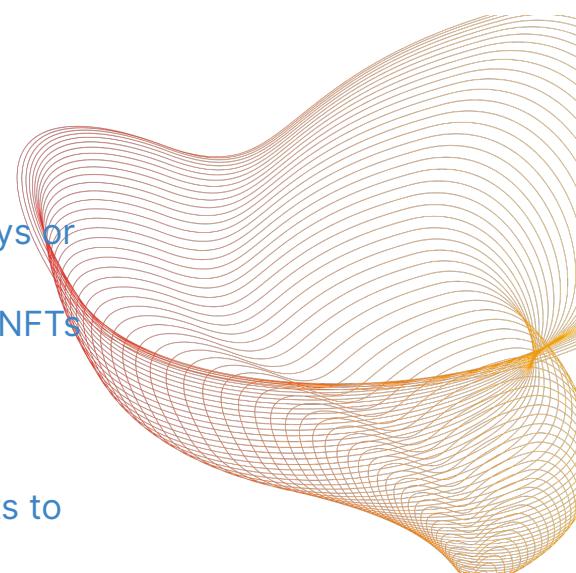
Mitigating NFT Investment Risks

- Thorough Research: Conduct comprehensive research before investing in NFTs.
- Diversify Investments: Spread investments across different NFTs and projects.
- Exercise Caution: Be cautious when transacting and carefully assess projects and platforms.
- Stay Informed: Keep up-to-date with the evolving NFT landscape and industry news.
- Due Diligence: Understand the projects behind NFTs and assess investment goals and risk tolerance.



Common Methods Used to Steal NFTs

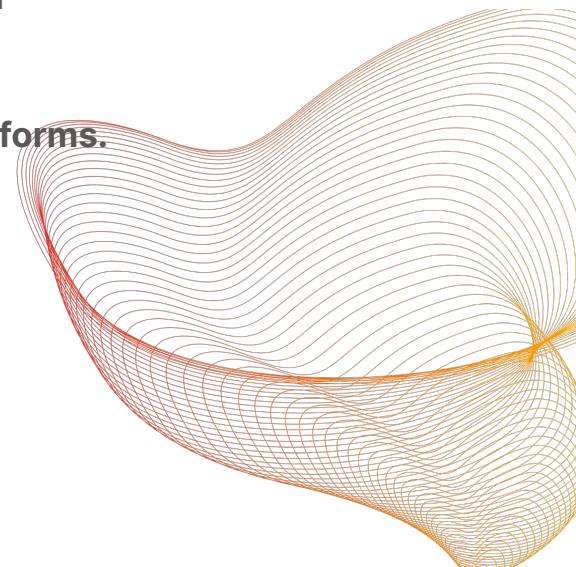
- **Minting Exploits:** Exploiting vulnerabilities in the minting process to create fake NFTs.
- **Phishing Attacks:** Impersonating legitimate websites or services to trick users into revealing private keys.
- **Smart Contract Vulnerabilities:** Exploiting vulnerabilities in smart contracts to steal NFTs.
- **Platform Hacks:** Gaining unauthorized access to platforms and transferring NFTs out of victims' wallets.
- **Social Engineering:** Manipulating users into giving away private keys or seed phrases.
- **Misconfigured Wallets:** Wallets with exposed private keys making NFTs susceptible to theft.
- **Third Party Tools and Services:** Malicious or vulnerable tools compromising the security of NFT holdings.
- **DNS Attacks:** Redirecting users to fake NFT marketplaces or wallets to steal private keys.





Protecting NFT Holdings Summary

- Use reputable wallets and marketplaces.
- Enable two-factor authentication (2FA) whenever possible.
- Be cautious of unsolicited messages and emails.
- Only share private keys or seed phrases with trusted and verified sources.
- Regularly update software and wallets to apply security patches.
- Perform due diligence when interacting with new projects or platforms.





Token Standards: ERC-721 and ERC-1155

Compare the differences between ERC-721 and ERC-1155.

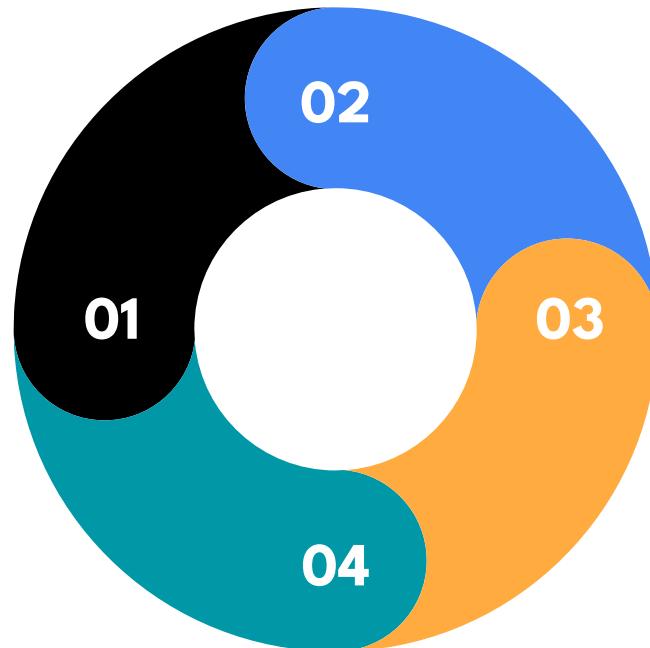
An overview of ERC-721 and ERC-1155 token standards and their differences



What is Zeppelin standard 721?

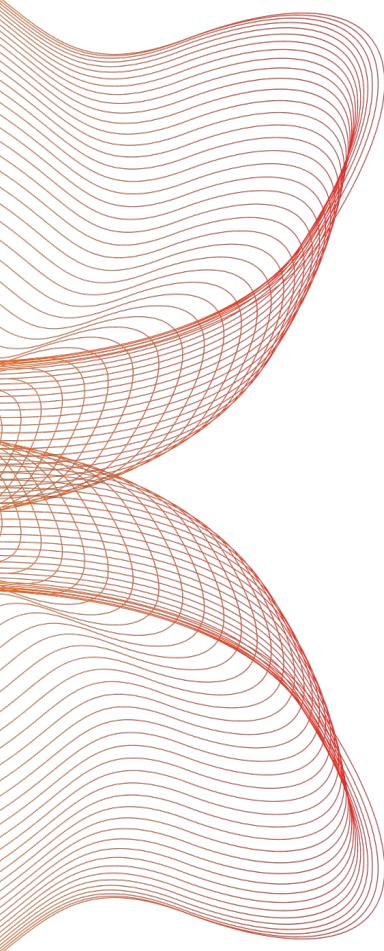
Zeppelin Standard 721 refers to Open Zeppelin's implementation of the ERC-721 standard

ERC-721 is a widely adopted standard for creating and managing non-fungible tokens (NFTs) on Ethereum



NFTs are unique digital assets representing ownership of specific items, content, or artwork

OpenZeppelin provides a development framework for secure and audited smart contracts, including ERC-721



What is Zeppelin standard 1155?

- ERC-1155 is a standard for multi-token contracts on Ethereum, allowing management of both fungible and non-fungible tokens
 - OpenZeppelin offers a secure and audited implementation of ERC-1155 for creating various types of tokens
- 



Comparison: ERC-721 vs ERC-1155

	ERC-721	ERC-1155
Token Type	Non-Fungible Tokens only	Fungible and Non-Fungible Tokens In a single contract
Efficiency	Higher deployment costs and storage	More efficient in gas costs and deployment
Batch Operations	Each transfer requires separate transaction	Supports batch operations for multiple tokens
Use Cases	Unique, indivisible items	Various token types
Flexibility	Less flexible for multiple token types	More flexible for different token types
Storage Efficiency	Redundancy in storage	Efficient use of blockchain storage space
Ecosystem Adoption	Well-established in art/collectibles space	Gaining popularity in gaming and diverse projects

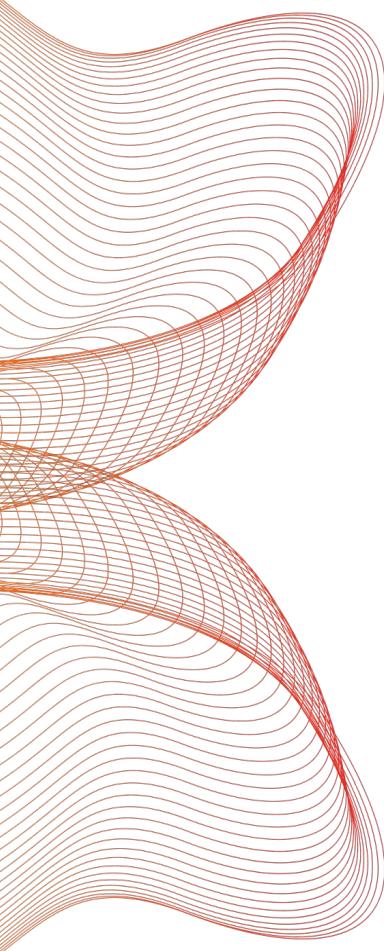


Non-EVM Blockchains and NFT Smart Contracts

**What are non-EVM blockchains offering regarding
NFT smart contracts?**

Explore the offerings of non-EVM blockchains with regards to NFT smart contracts.





Non-EVM Blockchains

Introduction

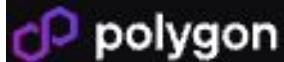
- 01** Several non-EVM blockchains now offer NFT smart contract functionality

 - 02** Non-EVM blockchains are expanding the NFT ecosystem beyond Ethereum
- 



Binance Smart Chain (BSC)

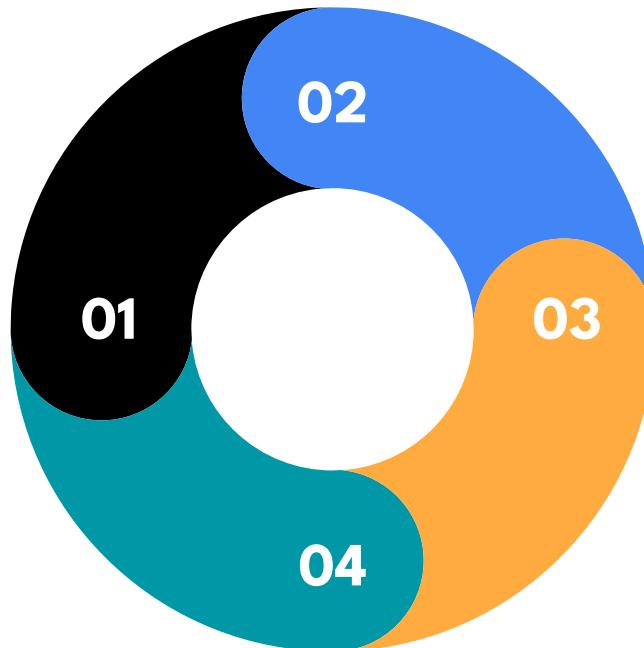
- BSC is a blockchain platform by Binance
- It supports smart contracts and is EVM compatible
- NFT functionality is available through smart contracts



Polygon (formerly Matic Network)

Polygon is a multi-chain scaling solution for Ethereum

It offers various blockchain networks



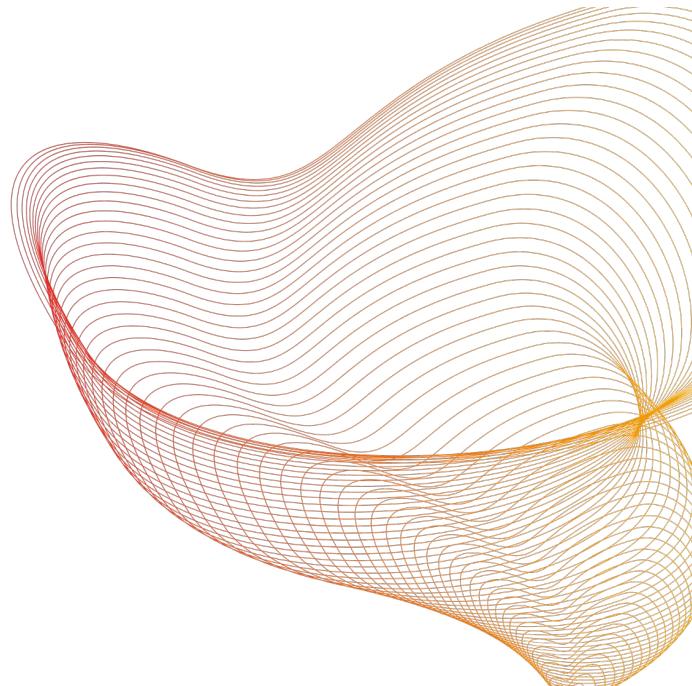
NFT smart contracts can be deployed on Polygon

Lower fees and faster transactions compared to Ethereum



Flow

- Flow is a blockchain built for NFTs and gaming applications
- Focuses on scalability and developer-friendly features
- Suitable for high throughput projects and smooth user experiences





WAX

WAX is a blockchain platform for trading virtual items and NFTs



User-friendly experience for developers and users

Popular within the gaming industry



Avalanche



- Avalanche provides high throughput and subsecond transaction finality
- Supports smart contracts and NFTs
- Offers diverse possibilities for developers





Tezos

Tezos is a self-amending blockchain platform



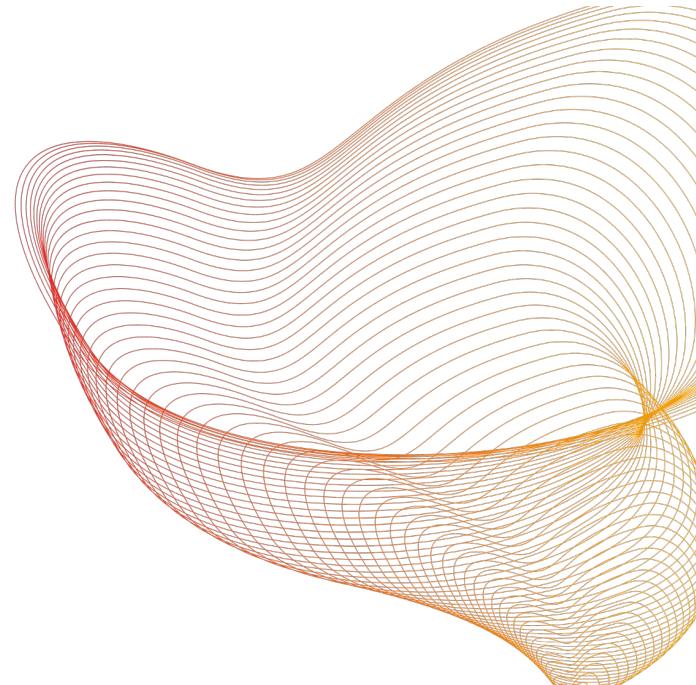
Create and manage NFTs directly on the Tezos blockchain

Supports smart contracts and its own NFT standards (e.g., FA2)



Solana

- Solana is a high performance blockchain platform
- Supports decentralized applications and NFTs
- Fast transaction speeds and low fees



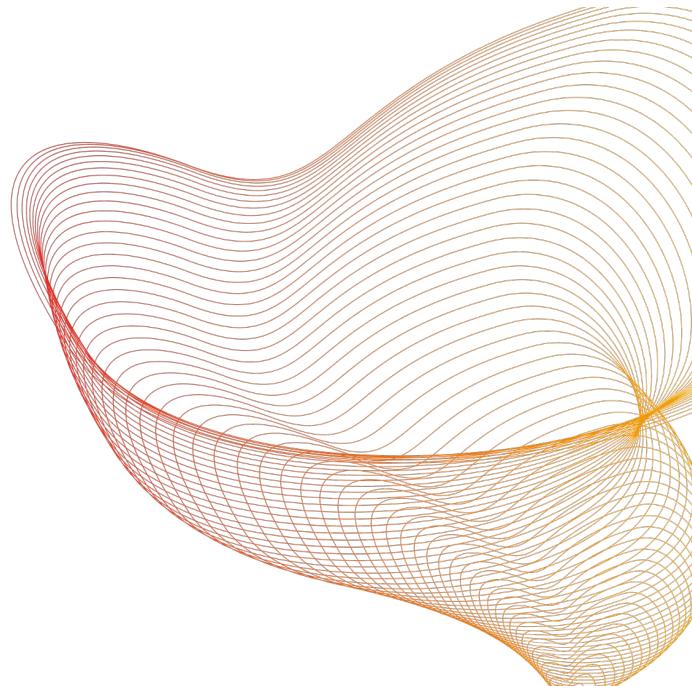
NEAR Protocol



- 01** Create and manage NFTs on the NEAR blockchain

- 02** NEAR is a user-friendly and scalable blockchain platform

- 03** Provides NFT support for developers





Hindrances of Blockchain for NFT Usability

What are the possible hindrances that a blockchain can pose for NFT usability?

This section highlights the possible hindrances that a blockchain can pose for NFT usability.



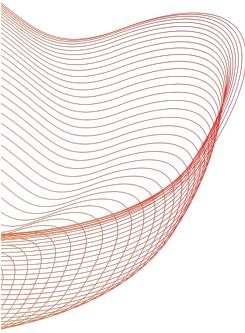


Scalability Issues

Blockchain networks can experience scalability limitations

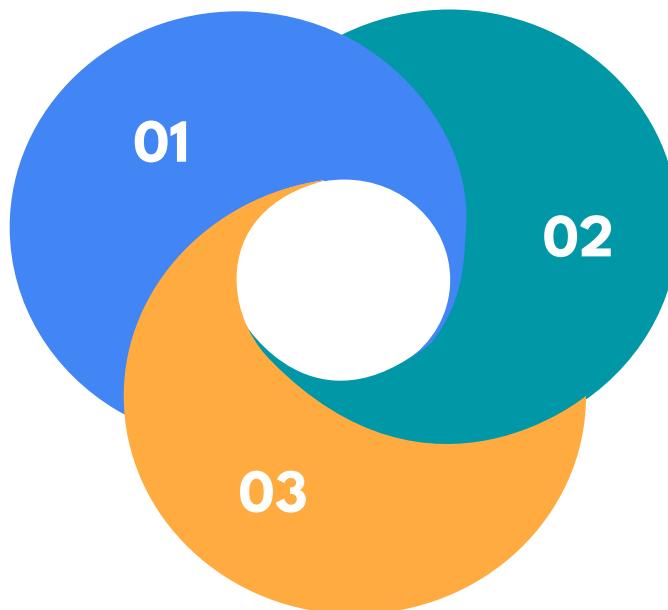
Congestion and slow transaction processing during peak usage times

Delays and high fees for NFT transactions



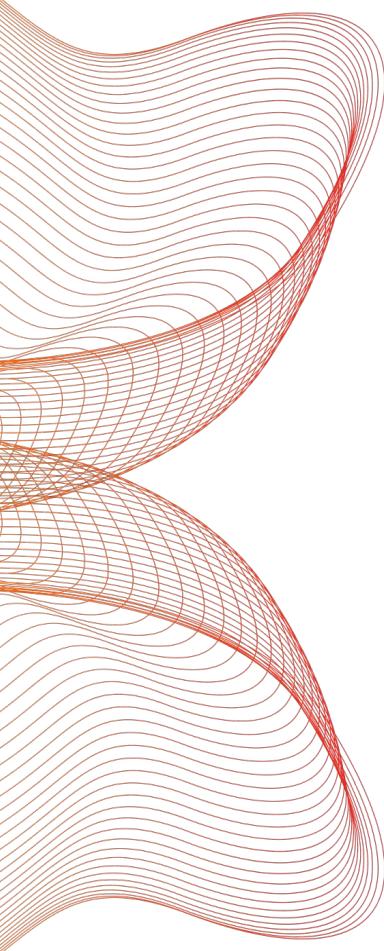
High Gas Fees

Blockchain networks require users to pay gas fees



Especially impacts lower-value items

Deters users from minting, buying, selling, or transferring NFTs

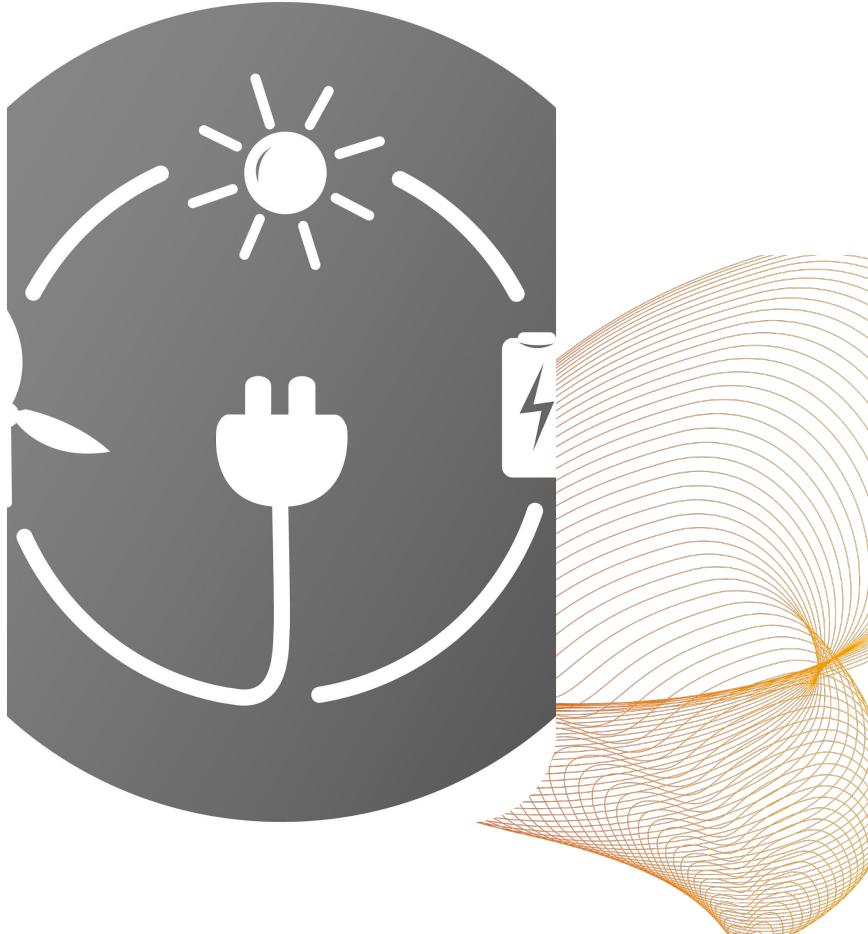


Complex User Experience

- Certain level of technical understanding required
 - Knowledge of wallets, private keys, and transaction processes
 - Discourages less tech savvy users from participating in the NFT ecosystem
- 

Environmental Concerns

- 01** Ethical concerns and negative public perception
- 02** Some blockchains have significant environmental impact
- 03** High energy consumption, especially with Proof of Work (PoW)



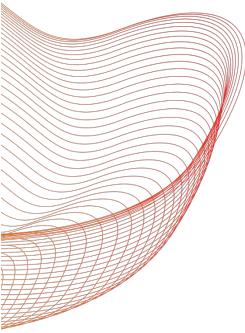


Interoperability Challenges

Different blockchains are not fully interoperable

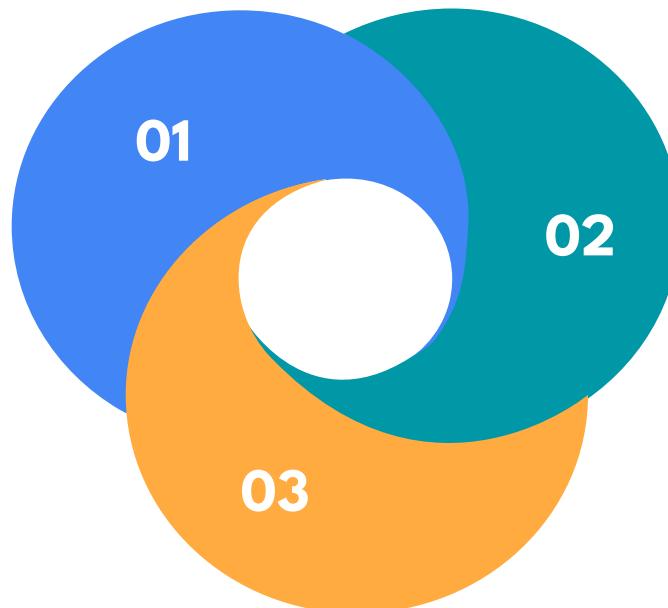
Difficult to transfer NFTs between networks

Hinders usability across various platforms



Limited File Storage

Restrictions on file sizes
on some blockchains



Requires off-chain storage
solutions

Limits the types of
media associated with
NFTs



Upgradeability Concerns

- Smart contracts governing NFTs may need upgrades or changes over time
- Impacts ownership and authenticity of existing NFTs

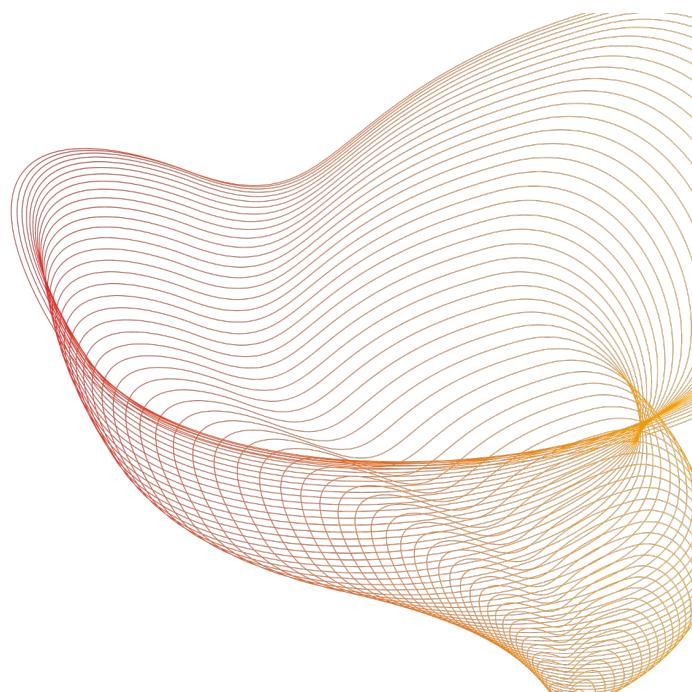


Lack of Regulation and Standards

01 Affects overall usability and adoption of NFTs

02 Lack of consistent regulations and standards in the NFT space

03 Uncertainty and disputes related to ownership and legal implications



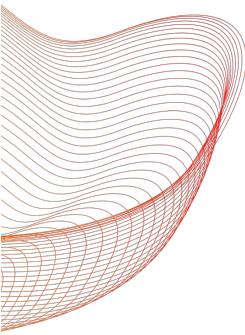


Privacy Considerations

Some blockchains prioritize transparency and public access to data

Impacts privacy of NFT holders and their transaction history

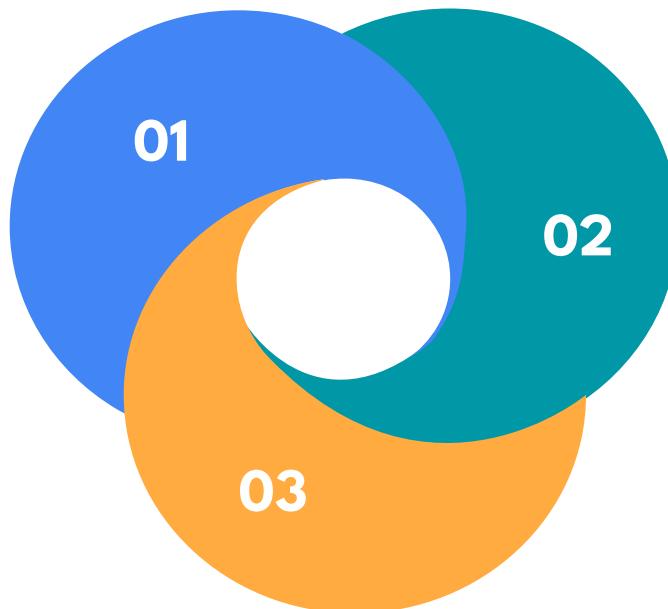
Discourages privacy-conscious users



Learning Curve

New users face a learning curve in the NFT ecosystem

Navigating blockchain technology



Setting up wallets,
managing private keys,
and understanding gas
fees

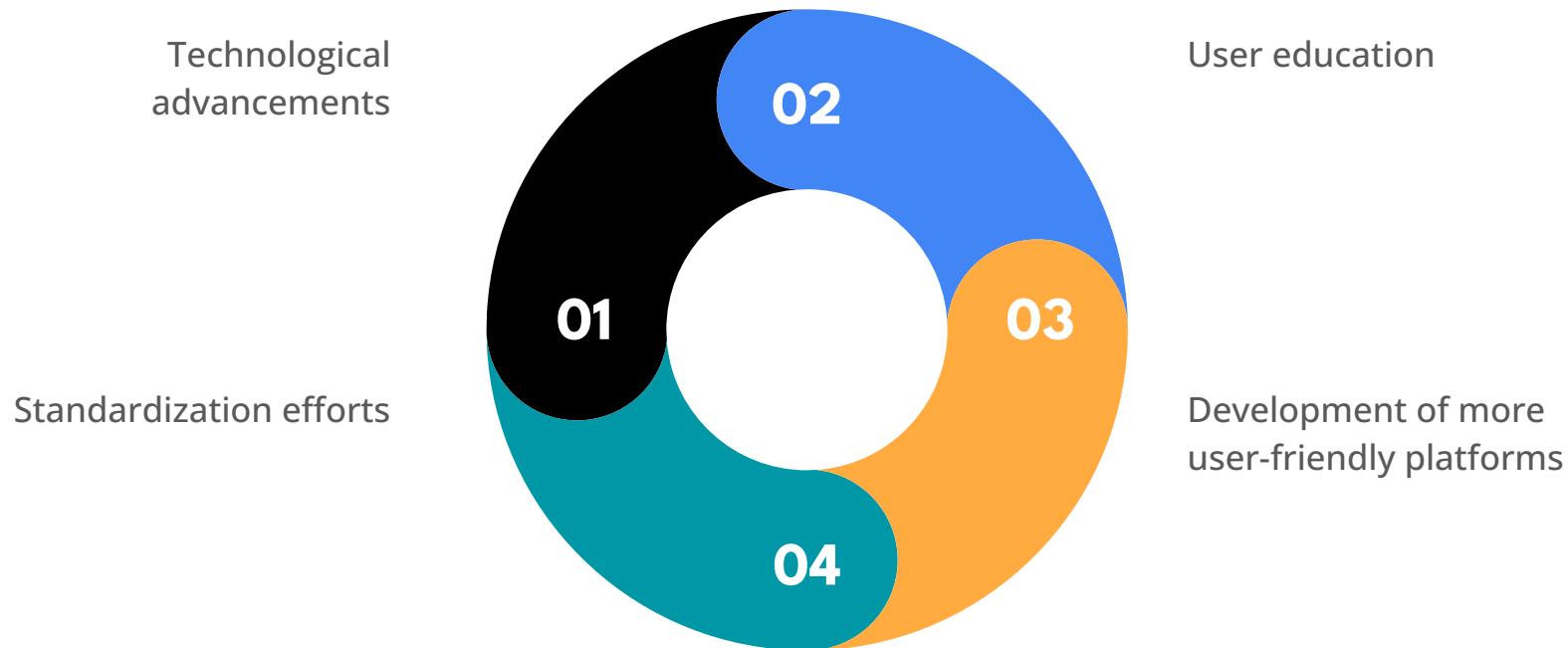


Platform Fragmentation

- NFT space characterized by various platforms
- Each with its own standards, wallets, and user interfaces
- Confuses users and complicates NFT discovery, buying, and management



Addressing Hindrances



Summary

- 01** Efforts are being made to address these hindrances

- 02** Hindrances can impact the usability of NFTs

- 03** Awareness of challenges is important for users and developers





Thank you. Please feel free to ask any questions. 😊