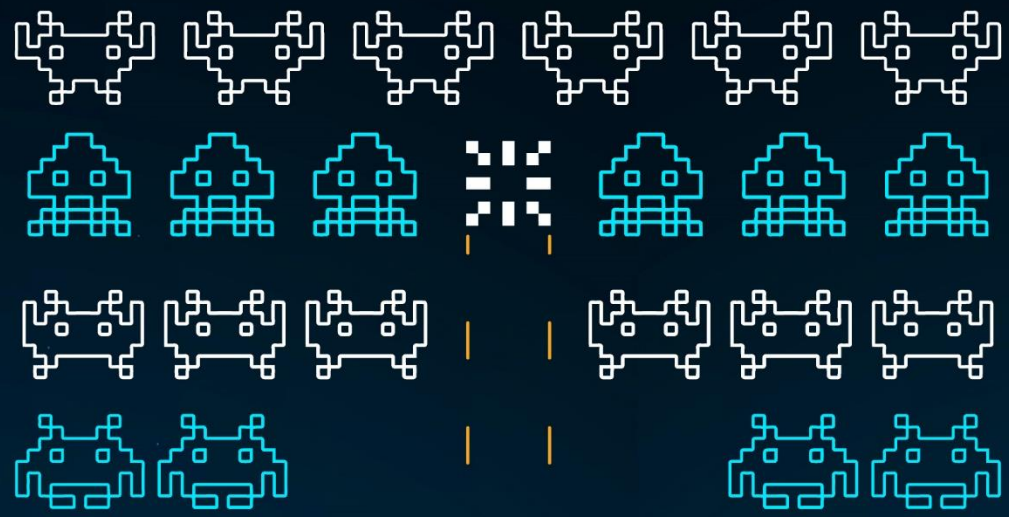
nccgroup

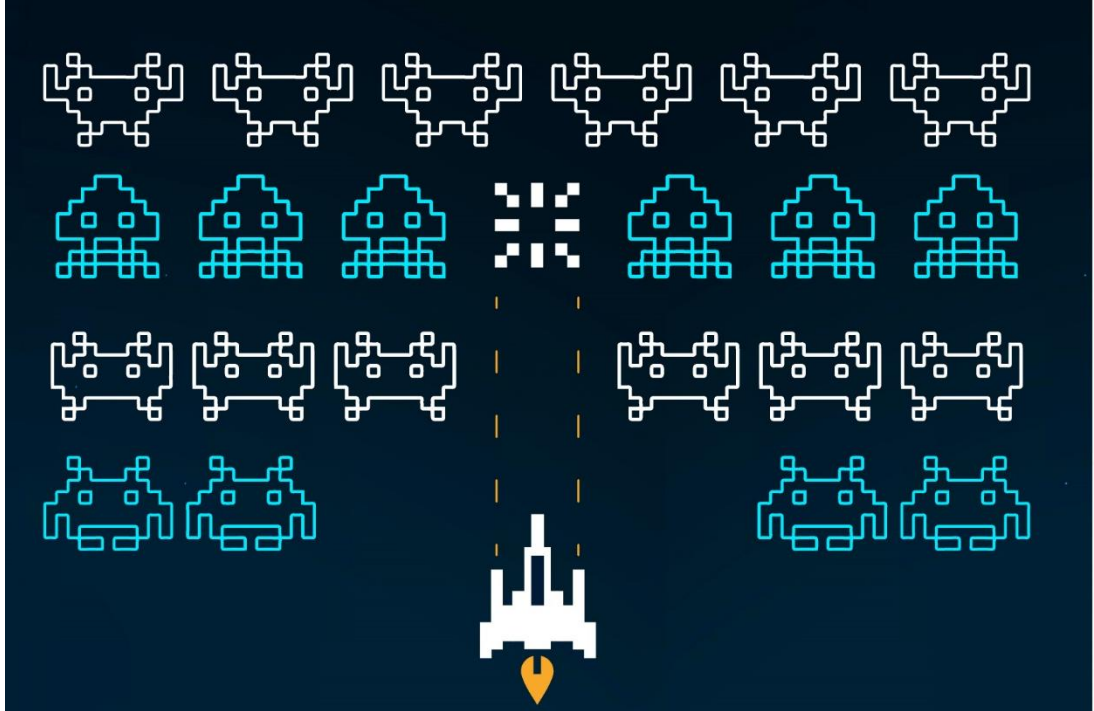
From Pixels to Profit: Mastering NFT Evaluation Strategies

Alejandra Ventura



WHOAMI

- Security consultant
- Member of the BlockSec Practice
- Certified Blockchain Security Professional (CBSP)

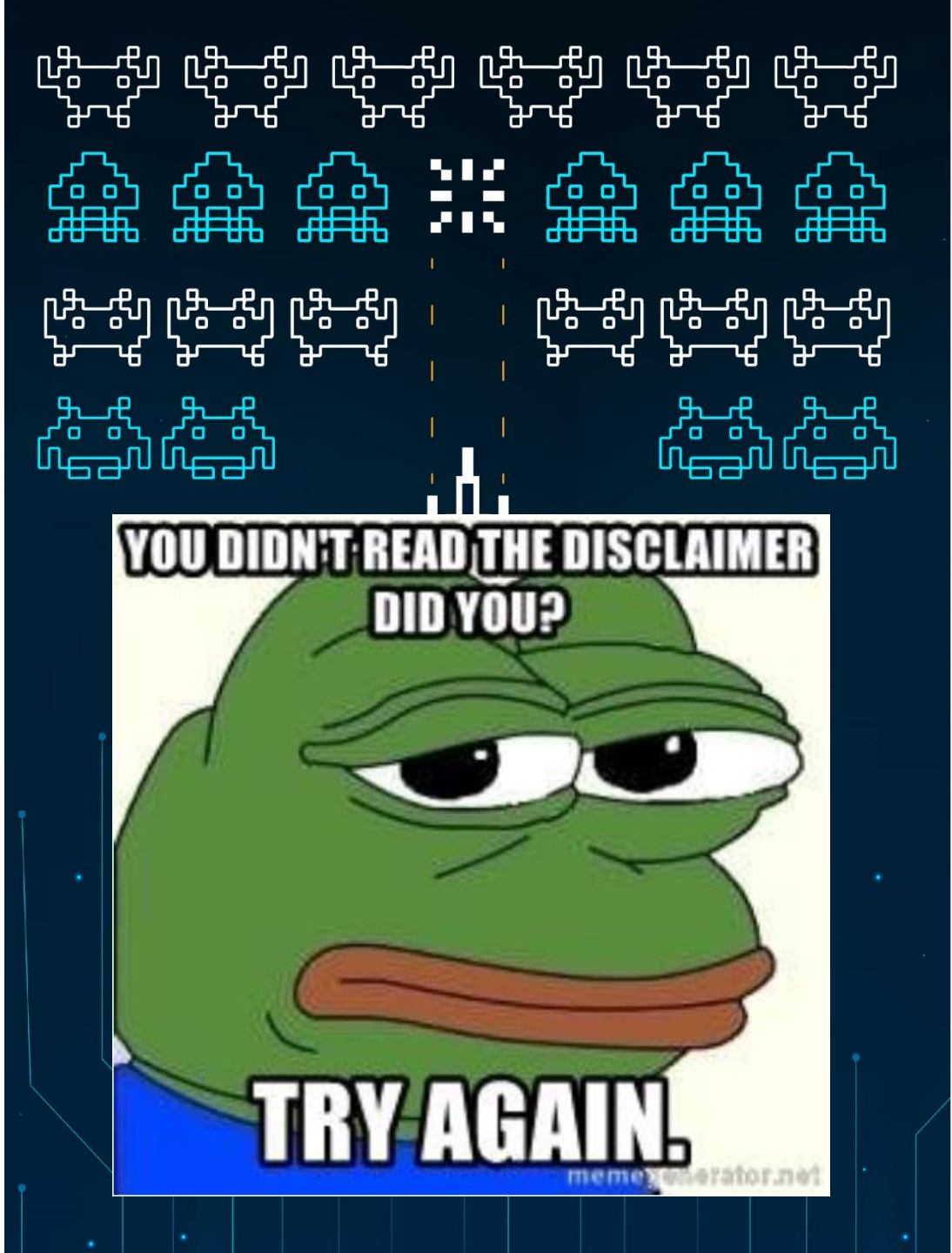


nccgroup

Alejandra Ventura

Disclaimer

- Due to the lack of time and for the sake of simplicity, some explanations will be skipped or just simplified.
- Some slides are based on images or text from other sources. Credit is given to external information sources.
- Keep in mind that I'm by no means an expert on NFTs.



Agenda

- What are NFTs?
- How do NFTs work?
- Common vulnerabilities
- Audit methodology
- Tools & NFTs IRL
- Interacting with NFT smart contracts
- Conclusion

Source: https://opensea.io/assets/ethereum/0x7e6027a6a84fc1f6db6782c523efe62c923e46ff/337785917162763915156958424035511712557990755532531214404460129035818981751 54

Non fungible tokens

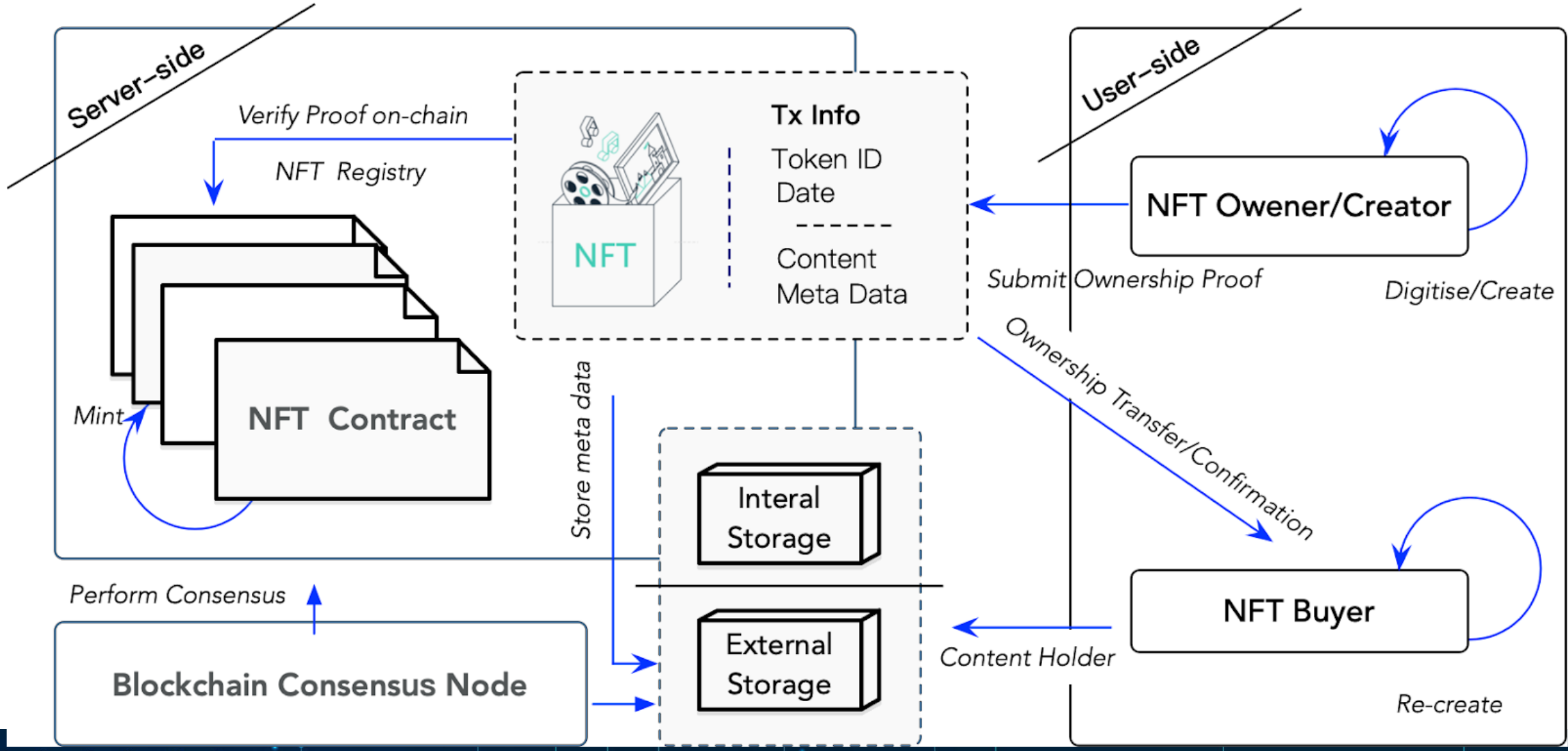
- **NFTs vs. Cryptocurrencies**

Topics	NFTs	Cryptocurrencies
Ownership	The owner of the NFT owns it with metadata, while the intellectual property belongs to the original artist. The owner could be the artist as well.	Similar to holding money. The holder entirely owns it.
Transactions	Can be modified and is minted through a smart contract. Minting an NFT means converting a file into a token so it's usable on a blockchain. The blockchain verifies the transaction, and charges a transaction fee.	Coins are "mined". A miner is a computer that performs an accounting function on the blockchain and they're paid in new coins.
Tradability	NFTs are non-fungible, and they have a value that goes way beyond economics.	Fungile (1 Crypto = Another Crypto).

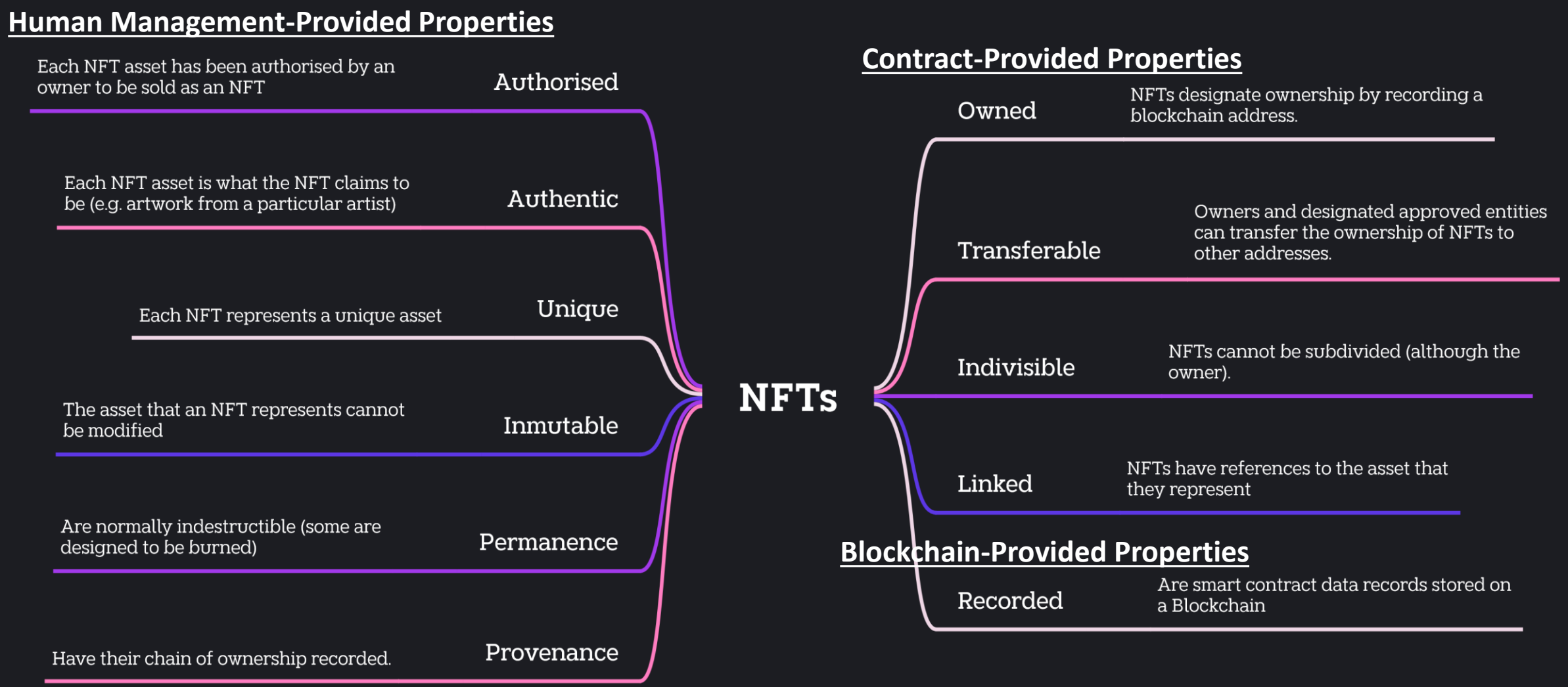
Image source: https://www.forbes.com/advisor/in/investing/what-is-an-nft-how-do-nfts-work/

A BRIEF HISTORY OF NFTS

How do NFTs work?



Source "Non-Fungible Token (NFT): Overview,Evaluation, Opportunities and Challenges." - Qin Wang, Rujia Li, Qi Wang, Shiping Chen.



Made with Chatmind

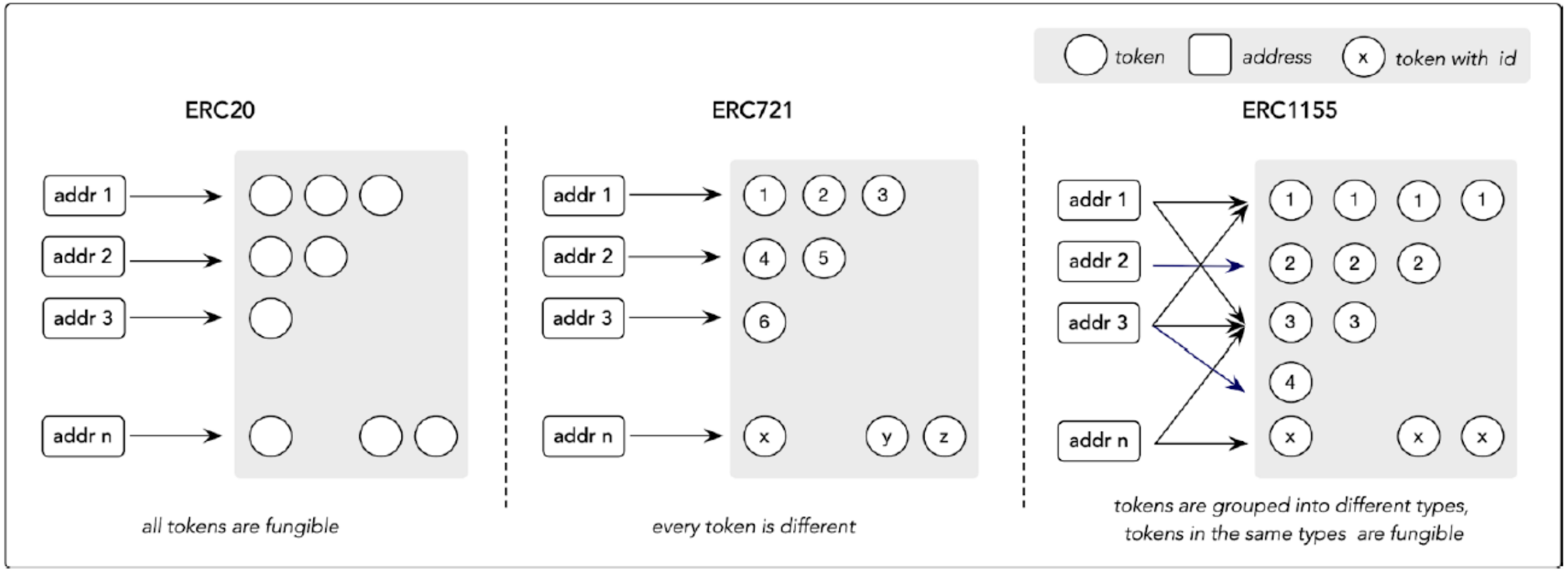
Attribute	Concerns
Owned	1. Misconception of asset ownership. 2. Unauthorized token creation linked to assets. 3. Vulnerability to account compromise and asset transfer by malicious actors. 4. Immediate sale of stolen tokens by malicious actors, hindering restoration.
Transferable	5. Lack of smart contract mechanisms for token restoration. 6. Potential misuse of restoration features by contract managers. 7. Possibility of adding restoration features, raising security concerns. 8. Vulnerability to theft due to coding errors.
Indivisible	9. Increased attack surface with fractional ownership. 10. Risk of loss through forced buyouts for fractional owners.
Linked	11. Risk of delinking from the asset due to inaccurate metadata. 12. Digital asset unavailability due to server errors. 13. Compromise of off-blockchain linking tables. 14. Potential misuse by table owners to delink or alter asset links.
Recorded	15. Public visibility of account and NFT ownership information. 16. Risk of de-anonymization through purchases linked with personal information.
Provenance	17. Potential for blockchain attacks altering history (though unlikely with established blockchains).
Permanence	18. Risk of NFTs being burned accidentally or maliciously. 19. Possibility of NFT smart contracts self-destructing.
Immutable	20. Vulnerability to changes in data records due to smart contract code vulnerabilities. 21. Blockchain modifications through consensus or splits, leading to issues like NFT duplication across chains.
Unique	23. Lack of awareness that an NFT might be sold multiple times. 24. Possibility of selling identical or nearly identical assets by multiple entities.
Authentic	25. Risk of linking NFTs to forged assets or misrepresenting the origin of authentic artworks.
Authorized	26. Unauthorized sale of NFTs by sellers. 27. Deception of buyers regarding the rights obtained over the linked asset.

NFT Security Risks

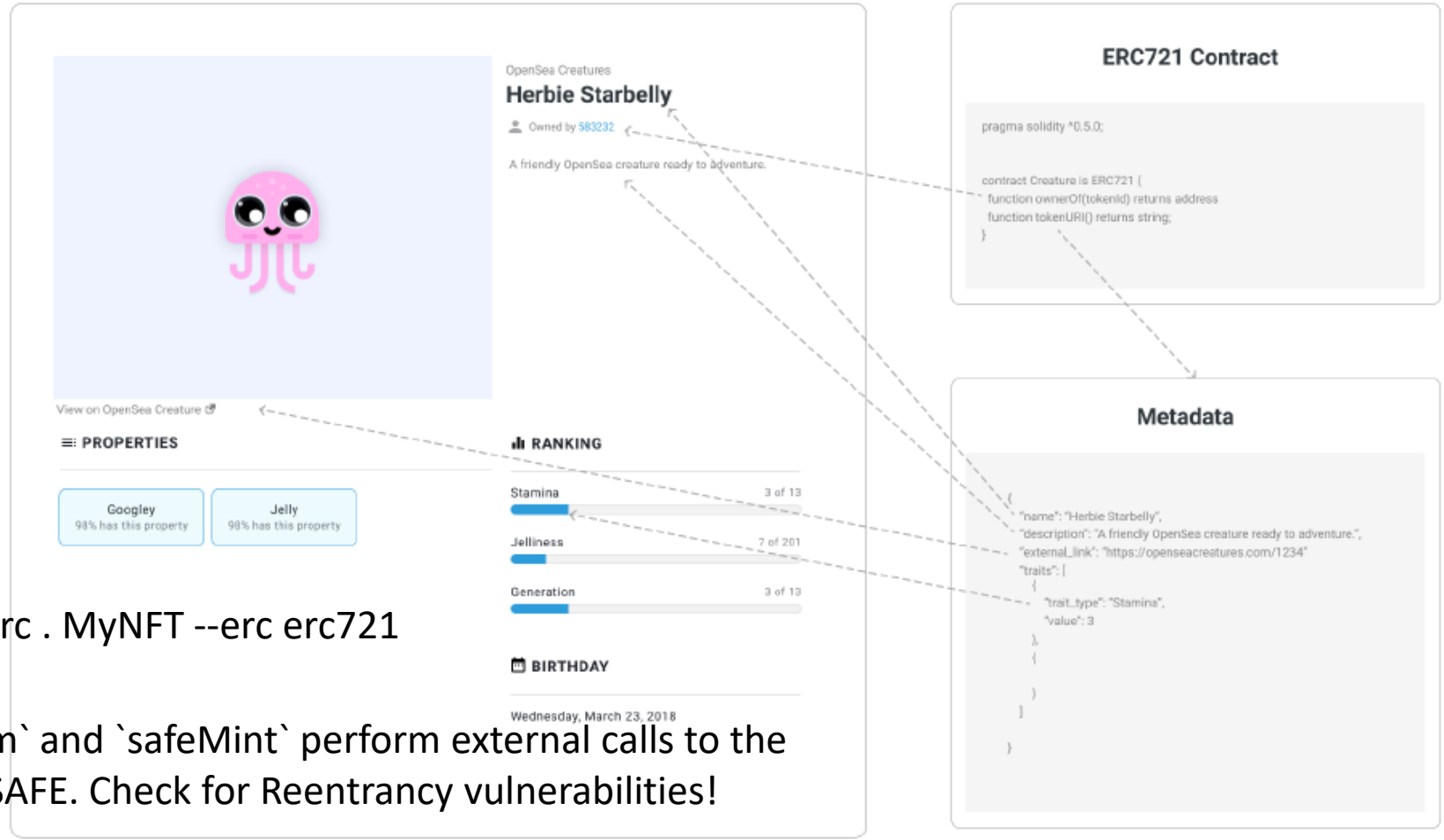
1. Marketplace risks
2. Mint exploits and smart contract vulnerabilities:
    1. Reentrancy
    2. Arithmetic Overflows and Underflows
    3. Default Visibilities
    4. Entropy Illusion
    5. Race Conditions
    6. Denial of Service (DOS)
    7. Constructors with Care
    8. Tx.Origin Authentication
3. Social engineering to steal private keys
4. Rug pulls (Scam)

nccgroup

Methodology - Network



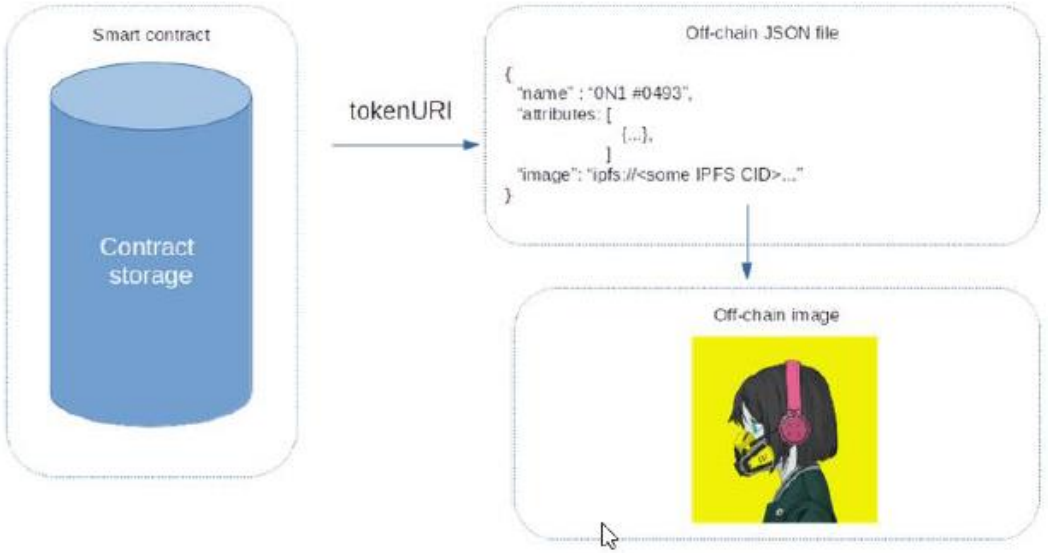
Methodology – Data Management



- slither-check-erc . MyNFT --erc erc721

• safeTransferFrom` and `safeMint` perform external calls to the receiver, are not SAFE. Check for Reentrancy vulnerabilities!

Methodology – Data Storage



Most NFT projects store their data elsewhere and only keep a link to it in their Smart contract. The SC provides a unique URI for each token, representing the ID of the NFT. This “ID” is like an address, pointing to where the NFT data is store.

Tools for Code review and analysis

Protocol Tools / Dev framework	Static Analysis	Decompiler / Disassembler	Visualization Tools	Dynamic Analysis
Ganache (Link)	Slither	Panoramix	Solgraph	MAIAN
Hardhat/Truffle	Mythrill	Heimdall-rs	Piet	Mythirll
Testnets → Goerli	MadMax	Ethervm	Etherscan	
Foundry / Brownie	Manticore / Rattle	Ethersplay	Surya	
	Sol2UML		Solidity Visual Developer	
Distros	**Fuzzing**	**ToolBox**	Test SM – Local Node	
Ziion	Echidna	Ethereum Security	Foundry/Anvil	
		Tool list (Consensys Tools) (Another link)		

Overview

Search

Smart Contract Weakness Classification (SWC)

- Overview
- SWC-100
- SWC-101
- SWC-102
- SWC-103
- SWC-104
- SWC-105
- SWC-106
- SWC-107
- SWC-108
- SWC-109
- SWC-110
- SWC-111
- SWC-112
- SWC-113
- SWC-114
- SWC-115
- SWC-116
- SWC-117
- SWC-118
- SWC-119
- SWC-120
- SWC-121
- SWC-122

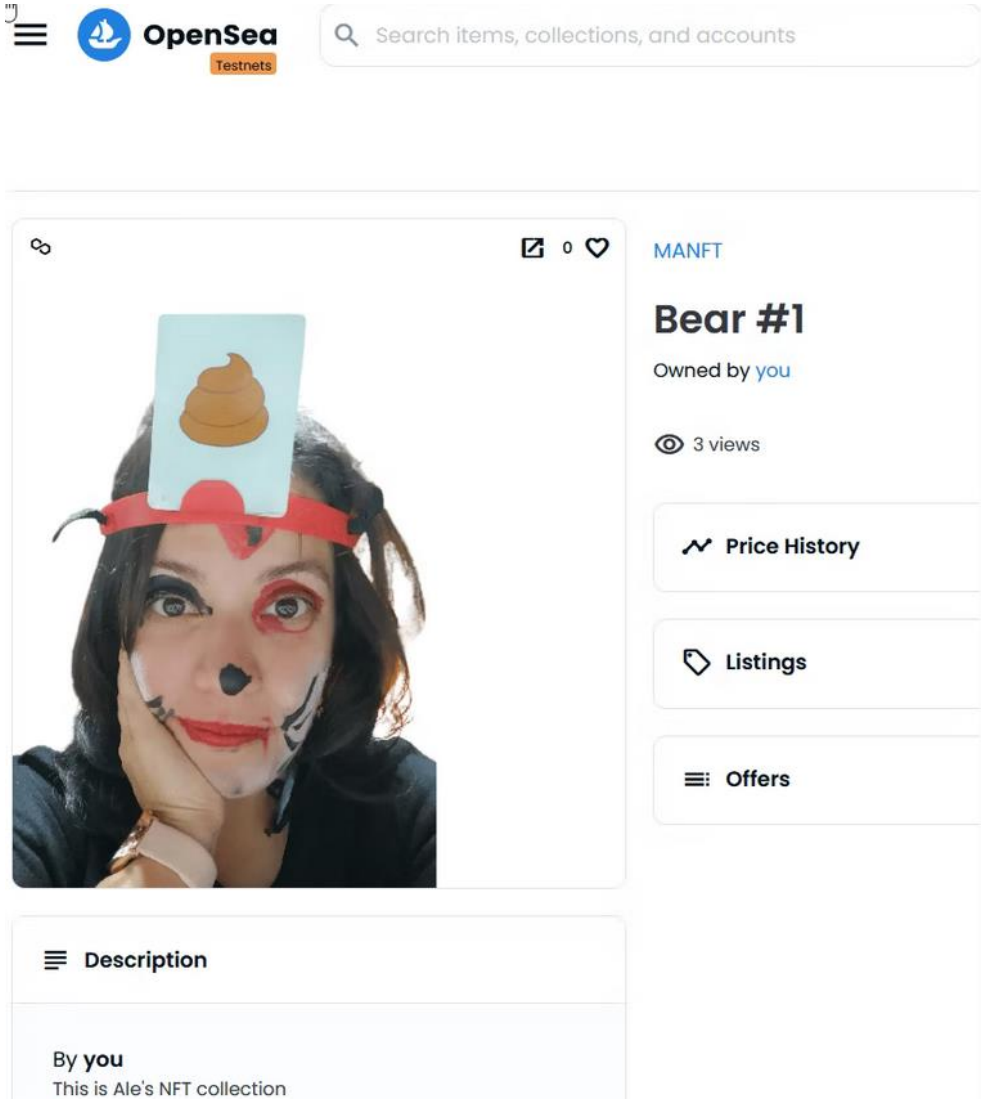
ID	Title	Relationships
SWC-136	Unencrypted Private Data On-Chain	CWE-767: Access to Critical Private Variable via Public Method
SWC-135	Code With No Effects	CWE-1164: Irrelevant Code
SWC-134	Message call with hardcoded gas amount	CWE-655: Improper Initialization
SWC-133	Hash Collisions With Multiple Variable Length Arguments	CWE-294: Authentication Bypass by Capture-replay
SWC-132	Unexpected Ether balance	CWE-667: Improper Locking
SWC-131	Presence of unused variables	CWE-1164: Irrelevant Code
SWC-130	Right-To-Left-Override control character (U+202E)	CWE-451: User Interface (UI) Misrepresentation of Critical Information
SWC-129	Typographical Error	CWE-480: Use of Incorrect Operator
SWC-128	DoS With Block Gas Limit	CWE-400: Uncontrolled Resource Consumption
SWC-127	Arbitrary Jump with Function Type Variable	CWE-695: Use of Low-Level Functionality
SWC-126	Insufficient Gas Griefing	CWE-691: Insufficient Control Flow Management
SWC-125	Incorrect Inheritance Order	CWE-696: Incorrect Behavior Order

https://swcregistry.io
https://github.com/transmissions11/solcurity

nccgroup

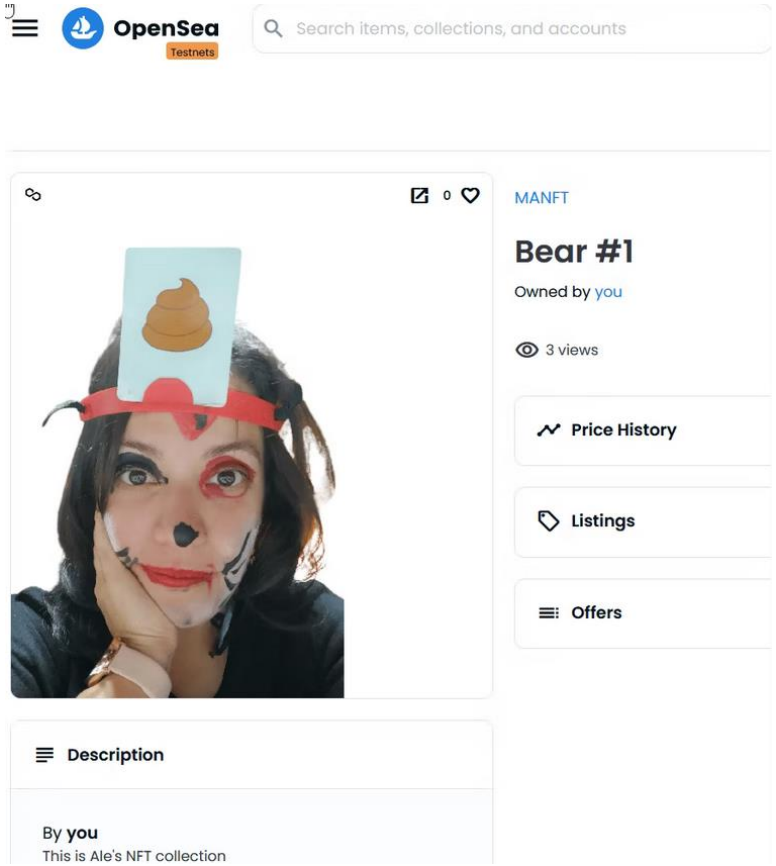
NFTs IRL

- NFT Smart Contract in Remix.
- Collection (OpenSea).
- NFT Smart Contract deployed (PolygonScan).
- CTF Smart Contract:
  - https://ethernaut.openzeppelin.com/
  - https://www.damnvulnerabledefi.xyz/
- Audit examples:
  - https://secureum.substack.com/p/audit-techniques-and-tools-101
  - https://blog.openzeppelin.com/fei-protocol-audit/
  - https://blog.openzeppelin.com/fei-audit-2/
  - https://github.com/transmissions11/solmate/blob/main/audits/v6-Fixed-Point-Solutions.pdf



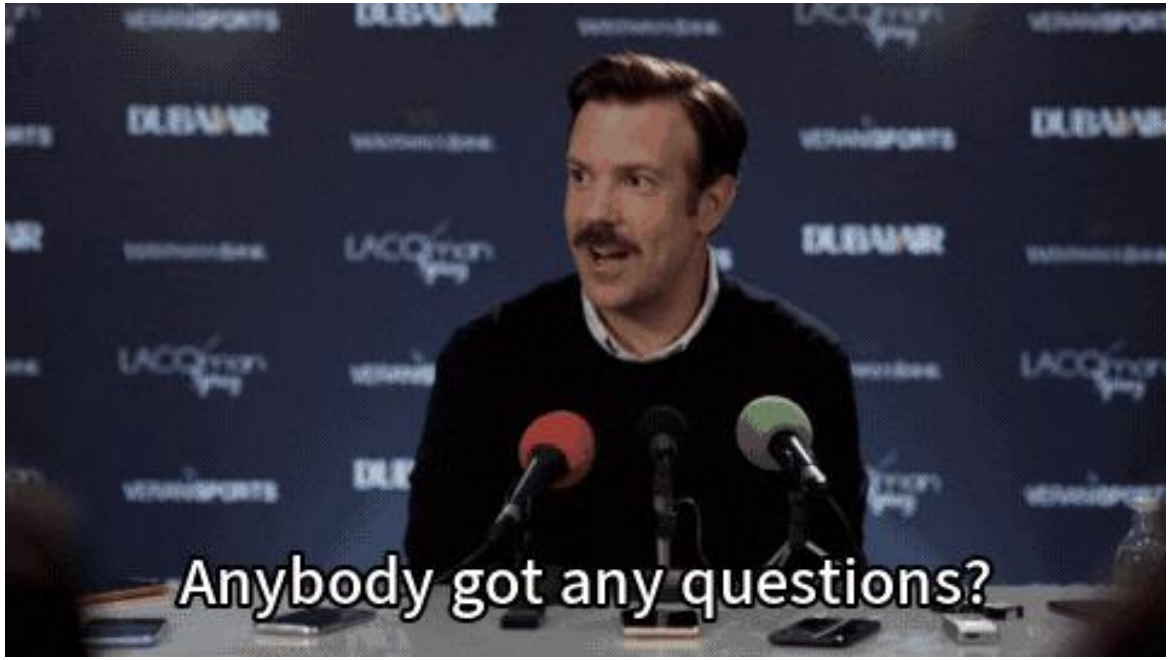
Interacting with NFT smart contracts

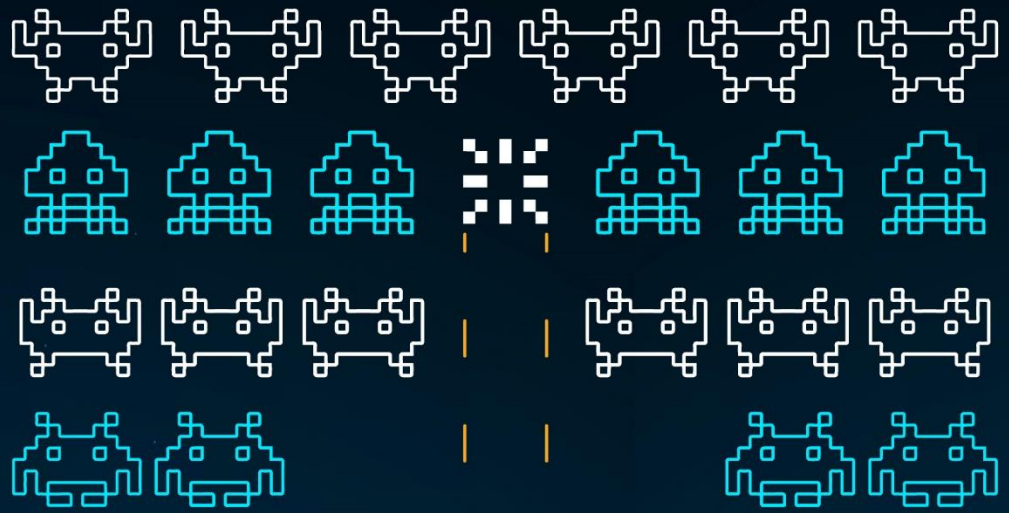
- Crypto wallet: Metamask.
- Network name: Mumbai
- New RPC URL: https://rpc-mumbai.maticvigil.com/
- Chain ID: 80001
- Currency symbol: MATIC
- Block explorer URL: https://mumbai.polygonscan.com/
- Send MATIC (Fake): https://mumbaifaucet.com/
- CTF - Fallback
- Remix Contract Fallback



Conclusion

- NFTs are at risk of theft through smart contract vulnerabilities and social engineering.
- Vulnerabilities can result in unauthorized mounting of NFTs, while social engineering can deceive users into transferring them to malicious addresses.
- Smart contract auditors are crucial in safeguarding NFTs through regular security assessments and recommendations for improvements.
- Users must remain updated on the latest security threats and take proactive measures to protect their NFTs from hacking.
- NFT reliance on blockchains and smart contracts provides secure cryptographic methods for establishing and publicly recording ownership. The NFT smart contracts provide the NFT properties of recorded, owned, transferable, indivisible, and linked. The blockchain ensures provenance, permanence, and immutable. Human NFT management provides the properties of unique, authentic, and authorized.





Many thanks!

alejandra.ventura@nccgroup.com
@venturita