



# You don't know NFTs (really!)



Kévin Lambert (*aka kvn*)  
Software Engineer @ Ledger

EthCC 22'



# What is an NFT ?



kvn's mom ♥

« It's a picture of bitcoin »



Someone who heard about it

« It's an image on the  
blockchain »



Someone who heard that it's  
not an image on the  
blockchain

« It's a proof of ownership »





# Is it an image on the blockchain ?



# Is it an image on the blockchain ?

- An NFT is mostly defined by metadata stored as a JSON
- Almost no NFT is actually stored on the blockchain for cost reasons
- Web2 storage (HTTP: Centralized)
- IPFS (P2P: Decentralized)

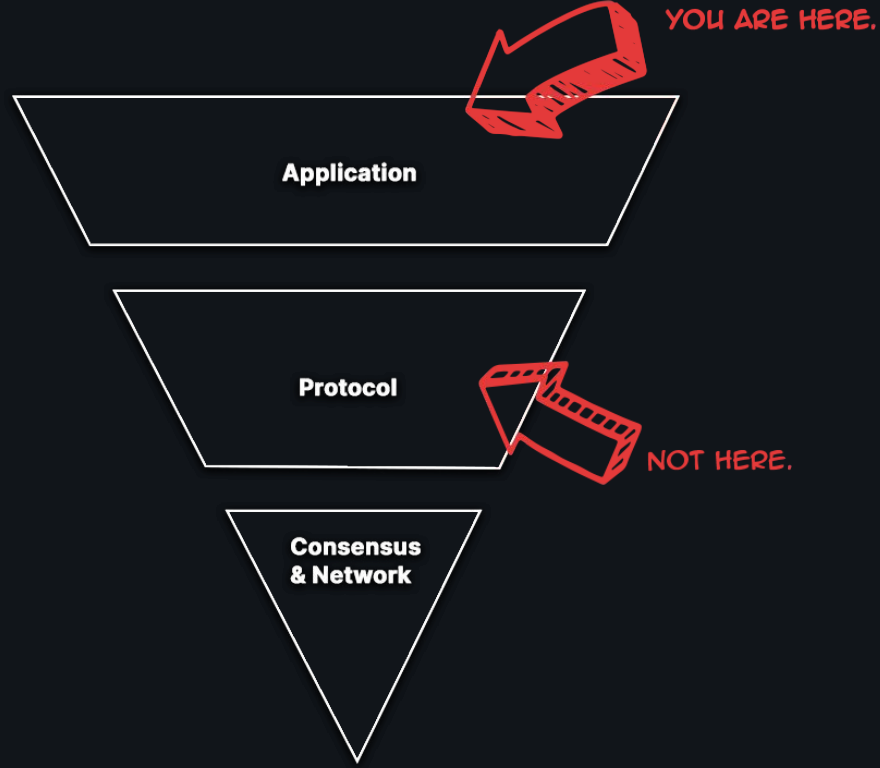


# Is it a proof of ownership ?



# Is it a proof of ownership ?

- Generally implies that NFTs are immutable
- Not true for Web2 storage
- Should be true for IPFS, right ?
- Who's the authority ?







# An NFT is just a string.

Using the ***tokenURI*** method with your NFT id will return the location of the metadata linked to it.

E.g.

**0xbc4ca0eda7647... (Bored Ape Contract)**

Calling the ***tokenURI*** method on the token id **1**

→ ***ipfs://QmeSjSinHpPnmXmspMjwiXyN6zS4E9zccariGR3jxcaWtq/1***

```
{
  "image": "ipfs://QmPbxGcXhYQQNgsC6a36dDyYUcHgMLnGKnF8pVFmGsvqi",
  "attributes": [
    {
      "trait_type": "Mouth",
      "value": "Grin"
    },
    ...
  ]
}
```

14. startingIndex →

15. startingIndexBlock →

16. supportsInterface →

17. symbol →

18. tokenByIndex →

19. tokenOfOwnerByIndex →

20. tokenURI ↓

tokenId (uint256)

1

Query

↳ string

[ tokenURI(uint256) method Response ]

» string :

***ipfs://QmeSjSinHpPnmXmspMjwiXyN6zS4E9zccariGR3jxcaWtq/1***



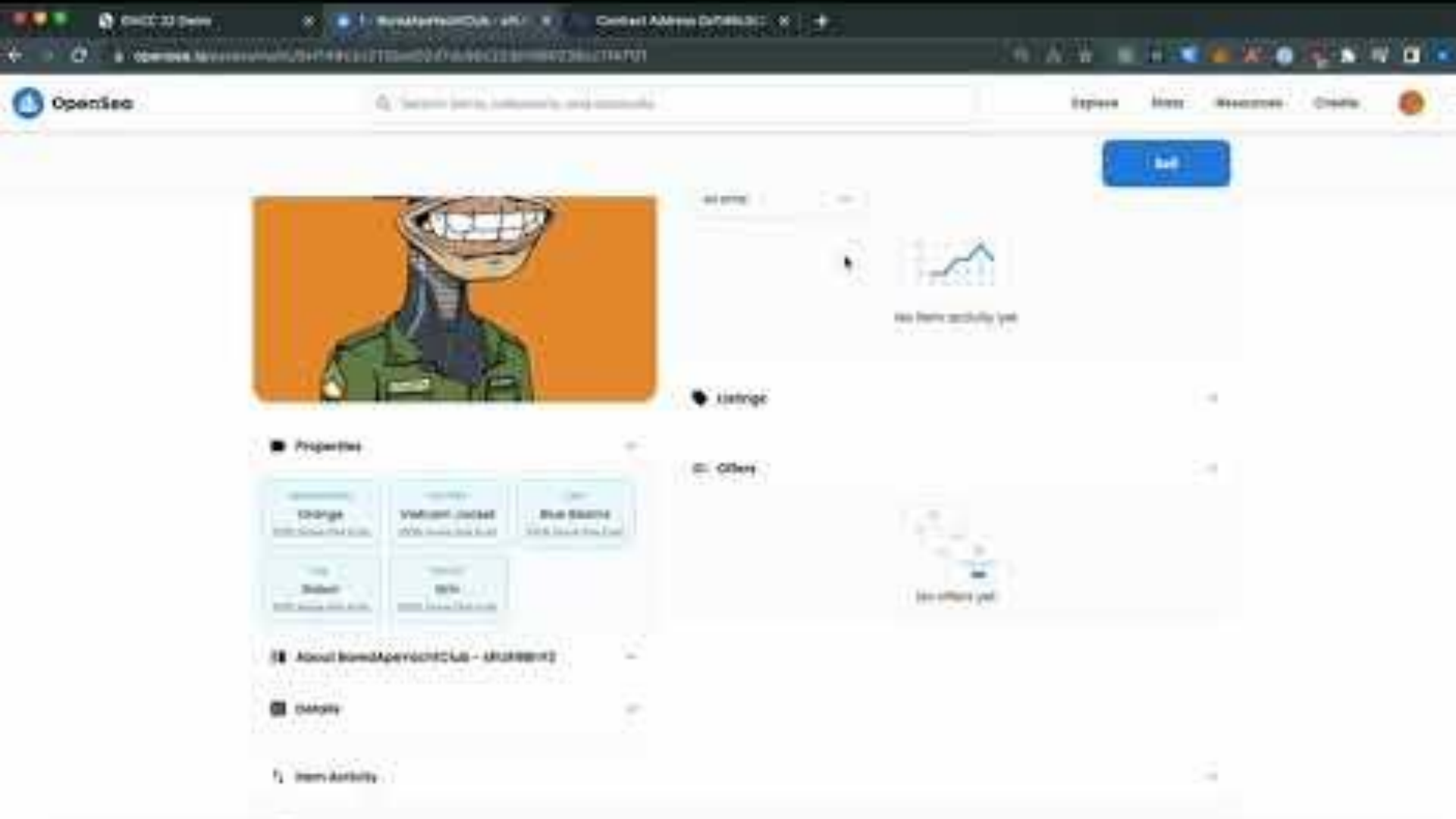
# This is string is immutable, right ?



# Nope.



# Code is Law. And here is an example



to contract 0xf149c3c2132ad00d76c60c223b1600235c79d71

You're viewing 1 NFTs

NFTs owned: 1 NFTs

Mint an NFT

Change  
Metadata

Transfer

Send Event

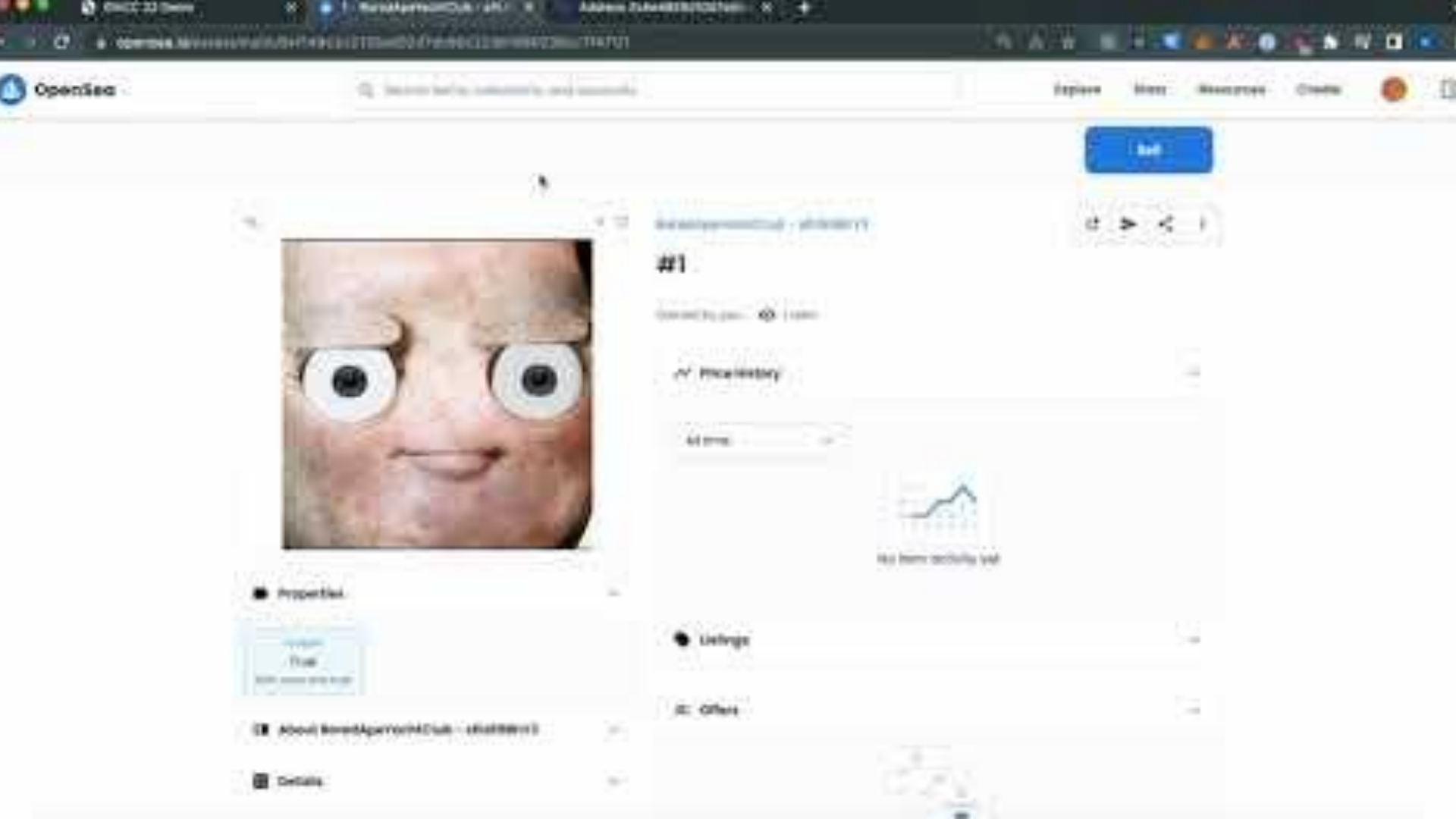


1st

<https://etherscan.io/tx/0x5000>

Transaction Hash: 0x5000

Block #1









You have no choice but  
to trust the owner.



# How can Ledger help me with that ?



# How can Ledger help me with that ?

- Clear signing for transfers in Ledger Live
- Ledger Market:
  - Clear signing for minting
  - Smart contract security review by The Donjon
  - Smart contract gouvernance by Ledger Vault
- You want all of that as well ? Ledger is an Open Platform !



# Thanks !

EthCC 22'