



Understanding Security Issues in the NFT Ecosystem

Dipanjan Das, Priyanka Bose,
Nicola Ruaro, Christopher Kruegel,
Giovanni Vigna

University of California, Santa Barbara

Presented at CCS 2022



The NFT frenzy



Search items, collections, and accounts

Explore

Stats

Resources

Create



Collection stats

The minimum price of an NFT in that collection

Top Trending Watchlist

All categories

All chains



1h

6h

24h

7d

30d

All

COLLECTION

1



Bored Ape Yacht Club

VOLUME

583 ETH

% CHANGE

+61%

FLOOR PRICE

77 ETH

SALES

8

% UNIQUE OWNERS

64%
6,411 owners

% ITEMS LISTED

7%
693 of 9,998



2



Mutant Ape Yacht Club

408 ETH

+16%

13.94 ETH

27

67%
12,953 owners

5%
1,037 of 19,425



3



Chromie Squiggle by Snowfro

362 ETH

+1,426%

12.50 ETH

28

28%
2,724 owners

2%
179 of 9,675



4



Otherdeed for Otherside

267 ETH

+7%

1.78 ETH

84

34%
33,868 owners

3%
3,290 of 100,000



5



Mint Pass Mexico City MPMX

259 ETH

+677%

1.50 ETH

41

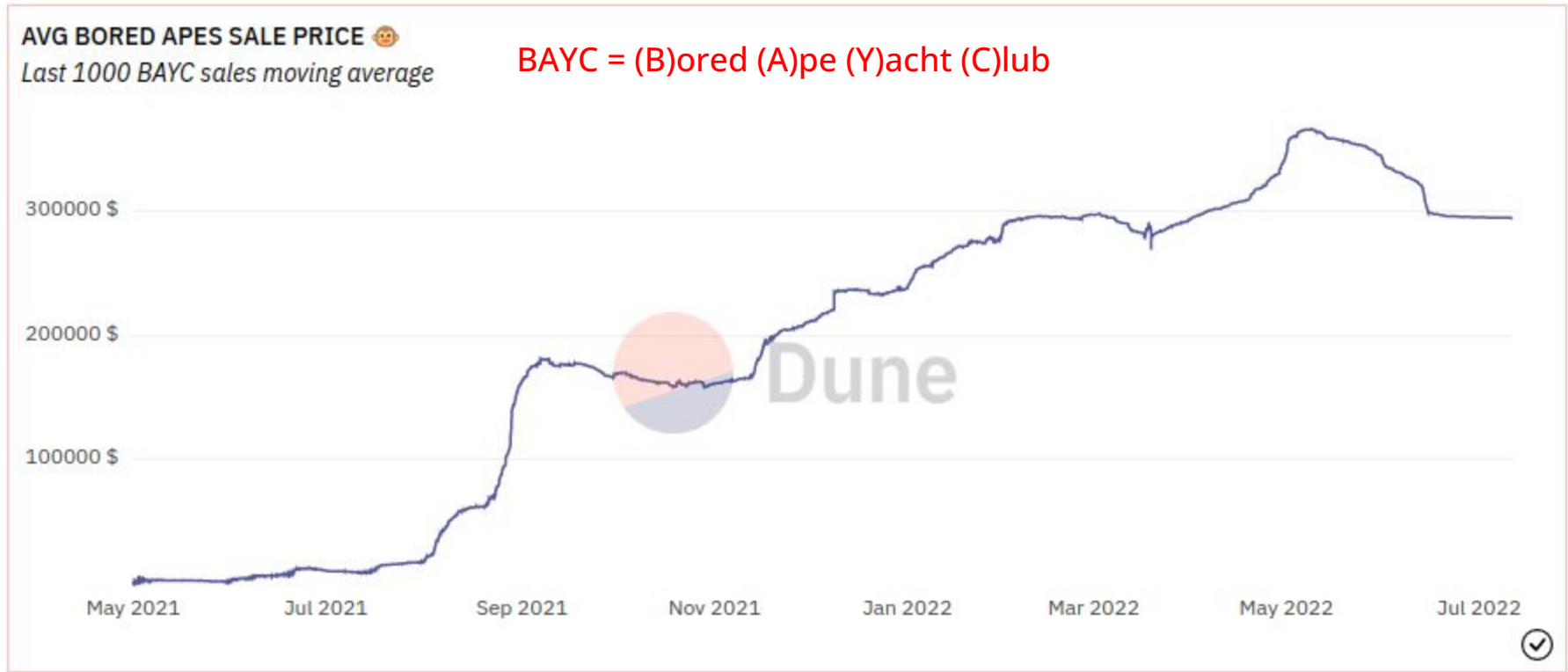
19%
186 owners

13%
126 of 1,000



Source: https://opensea.io/rankings?sortBy=one_day_volume, Date: October 13, 2022

The NFT frenzy



NFT hacks

CRYPTO / NFTS / TECH

\$1.7 million in NFTs stolen in apparent phishing attack on OpenSea users

NFTs Are Mysteriously Disappearing, Here's How

Keep an eye on your NFTs or they may vanish before you know.

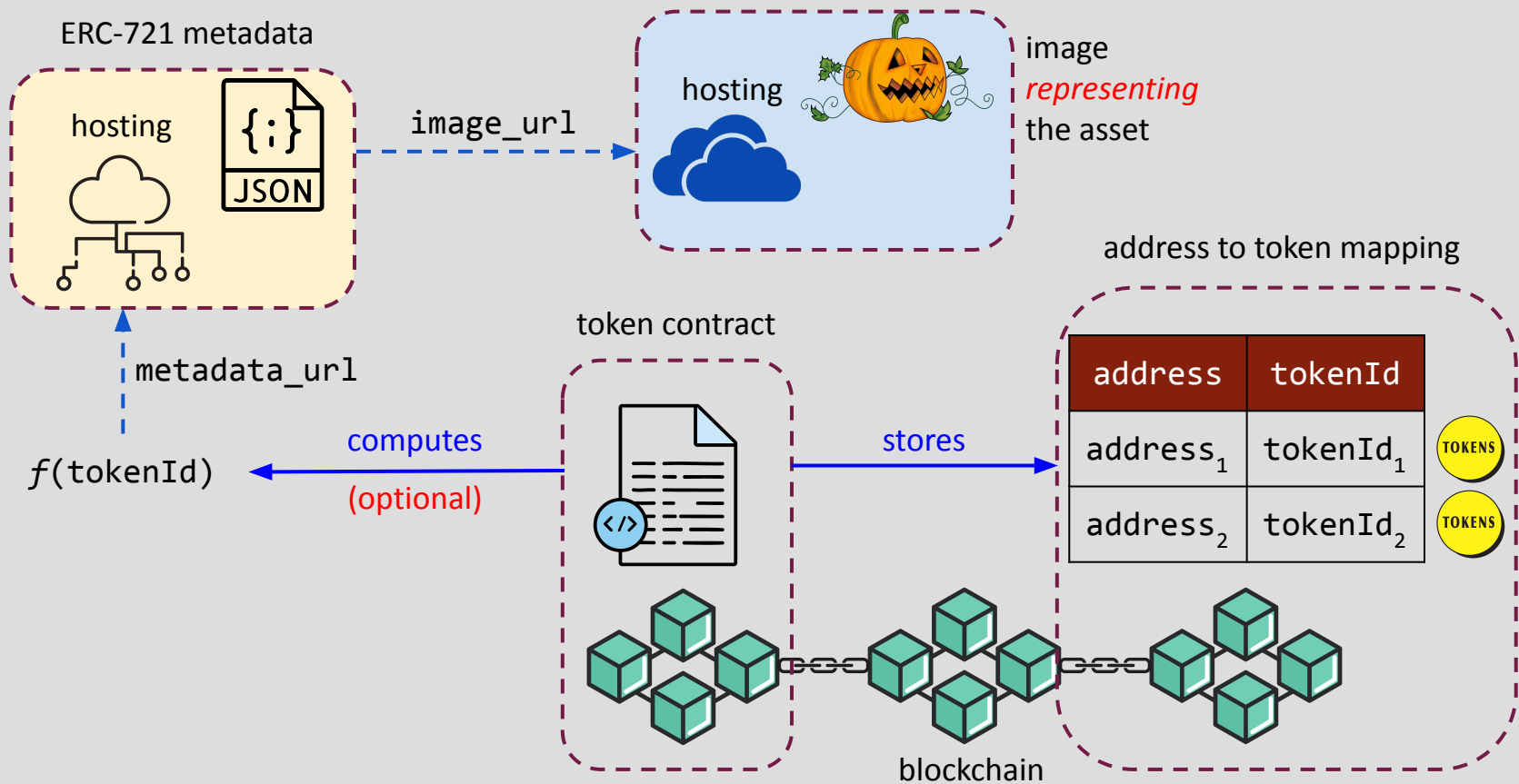
300+ NFTs Stolen, \$400K in Ethereum Taken In Premint Hack

Hackers infiltrated the popular NFT registration platform and used a fake pop-up to coerce users into giving up their wallet information.

"Our analysis is ongoing, but our initial assessment indicates that the impact was limited, none of the impacted accounts had 2FA enabled, and access was obtained via valid account credentials."

Two hundred and fifty-four tokens were stolen over roughly three hours

Non-Fungible Token (NFT)



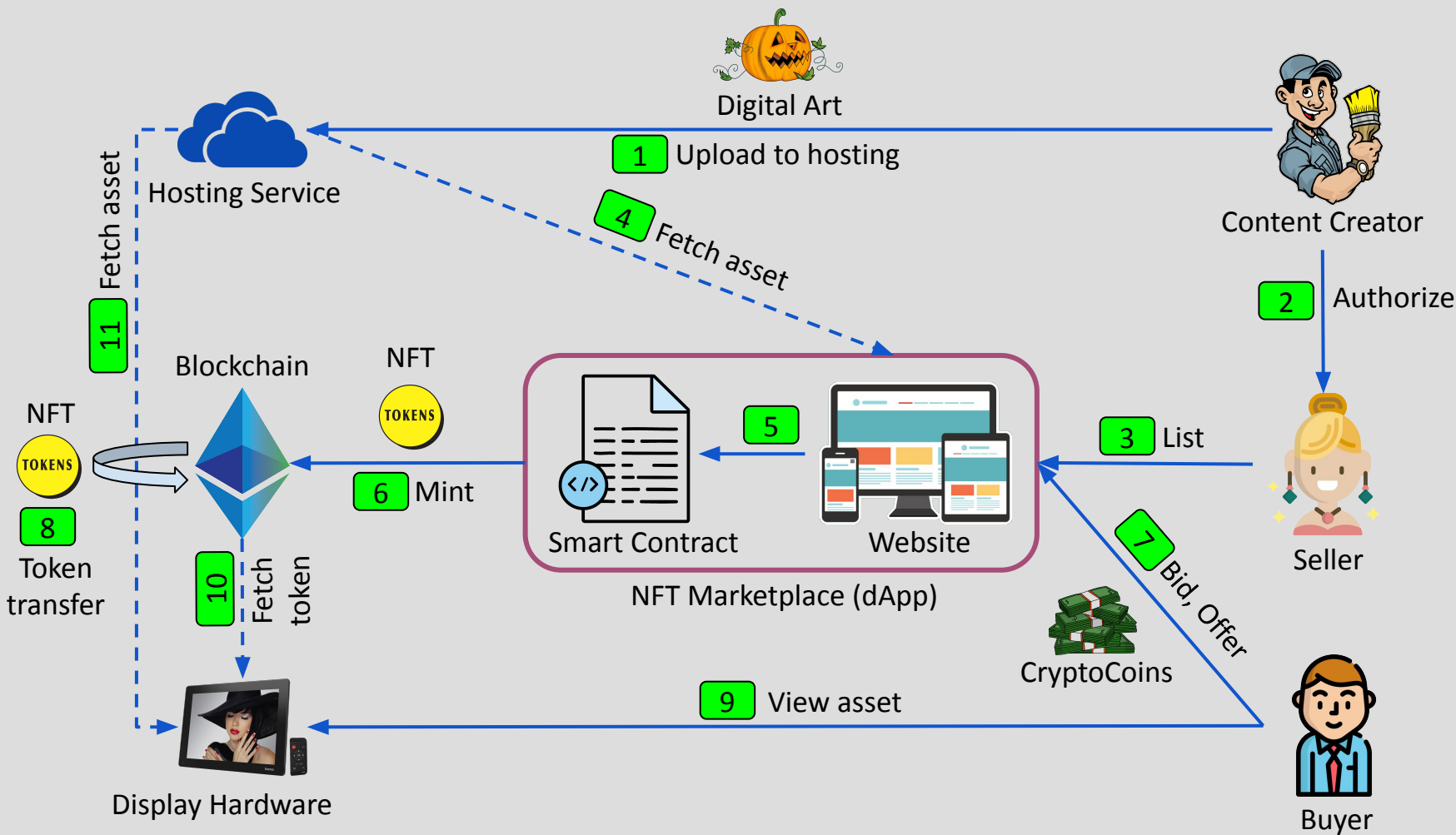
ERC-721 standard

`tokenURI(tokenId)` → Returns the `metadata_url` associated with the `tokenId`

`transferFrom(from, to, tokenId)` → Transfers the token with `tokenId` from the `from` address to the `to` address

`approve(controller, tokenId)` → Owner (`msg.sender`) authorizes the `controller` address to operate on the token with `tokenId`

`setApprovalForAll(operator, approved)` → Owner (`msg.sender`) delegates the authority of all of her tokens to the `operator` address



Actors in the ecosystem

External entities



Hosting Service



Display Hardware

Users



Content Creator



Seller



Buyer



Smart Contract



Website

NFT Marketplace (NFTM)

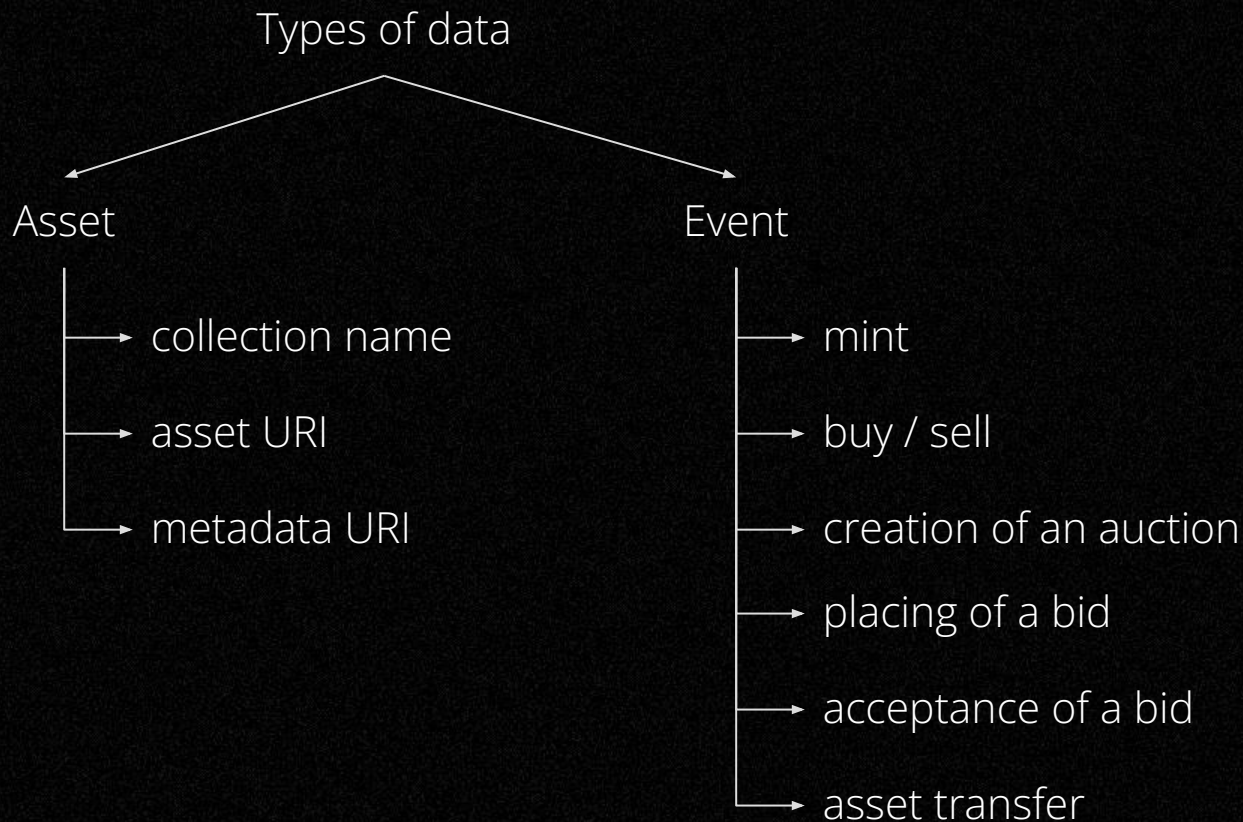
Marketplace selection

- Listed on DappRadar, a popular tracker for dApps
- Backed by Ethereum blockchain
- Total trading volume is over 50M USD as on June 15, 2021




Selected **8** out of 35 marketplaces
listed in DappRadar

Data collection



Data collection

- *API access*, if available
- *Web scraping*, if not prohibited by terms & conditions
- *Blockchain parsing*, if assets / events are visible from the blockchain
- *Otherwise*  for example, Nifty gateway



Data collection



OpenSea

Volume: 4.32B
Assets : 12.2M
Events : 349M

SuperRare

SuperRare

Volume: 107M
Assets : 28.6K
Events : 199K



CryptoPunks

Volume: 1.18B
Assets : 10K
Events : 172K



Rarible

Volume: 199M
Assets : 72.5K
Events : 1.8M



Axie

Volume: 1.75B
Assets : 891K
Events : 487K



sorare

Sorare

Volume: 97.4M
Assets : 298K
Events : 1.4M



Foundation

Volume: 68.2M
Assets : 112K
Events : 508K



Nifty

Volume: 300M
Assets : —
Events : —

Data collection



OpenSea

Volume: 4.32B
Assets : 12.2M
Events : 349M

- ✓ Had **18.2M** assets listed in OpenSea website at the time of crawling
- ✓ Crawled **66.94%** of the size of the marketplace
- ✓ OpenSea accounts for **89.63%** of assets in our dataset
- ✓ We use only OpenSea data unless the study requires cross-NFTM analysis



Issues in marketplaces

User authentication→Identity verification

- ★ NFTs can be used for money laundering
- ★ Major financial institutions have KYC (Know Your Customer) / AML (Anti-Money Laundering / CFT (Combating the Financing of Terrorism) policies in place
 - ✓ Banks
 - ✓ Brokerages
 - ✓ Crypto exchanges
 - ✗ NFT marketplaces (NFTMs)

Why are NFTMs exempted?



User authentication→Two-factor authentication

★ Authentication workflows

- Signature-based
- Password-based
 - 2FA adds extra layer of security

★ For NFT marketplaces with password-based authentication, 2FA is

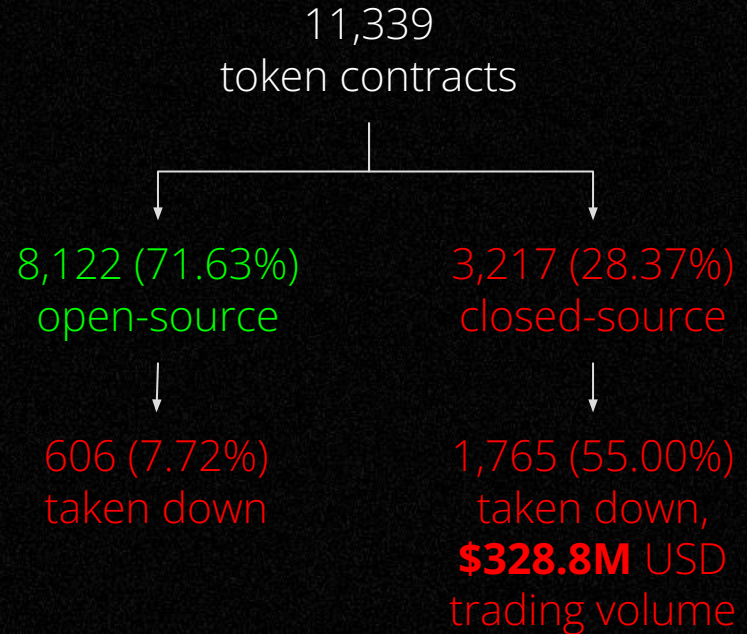
- either non-existent
- or, disabled by default

Nifty hack, March 2021

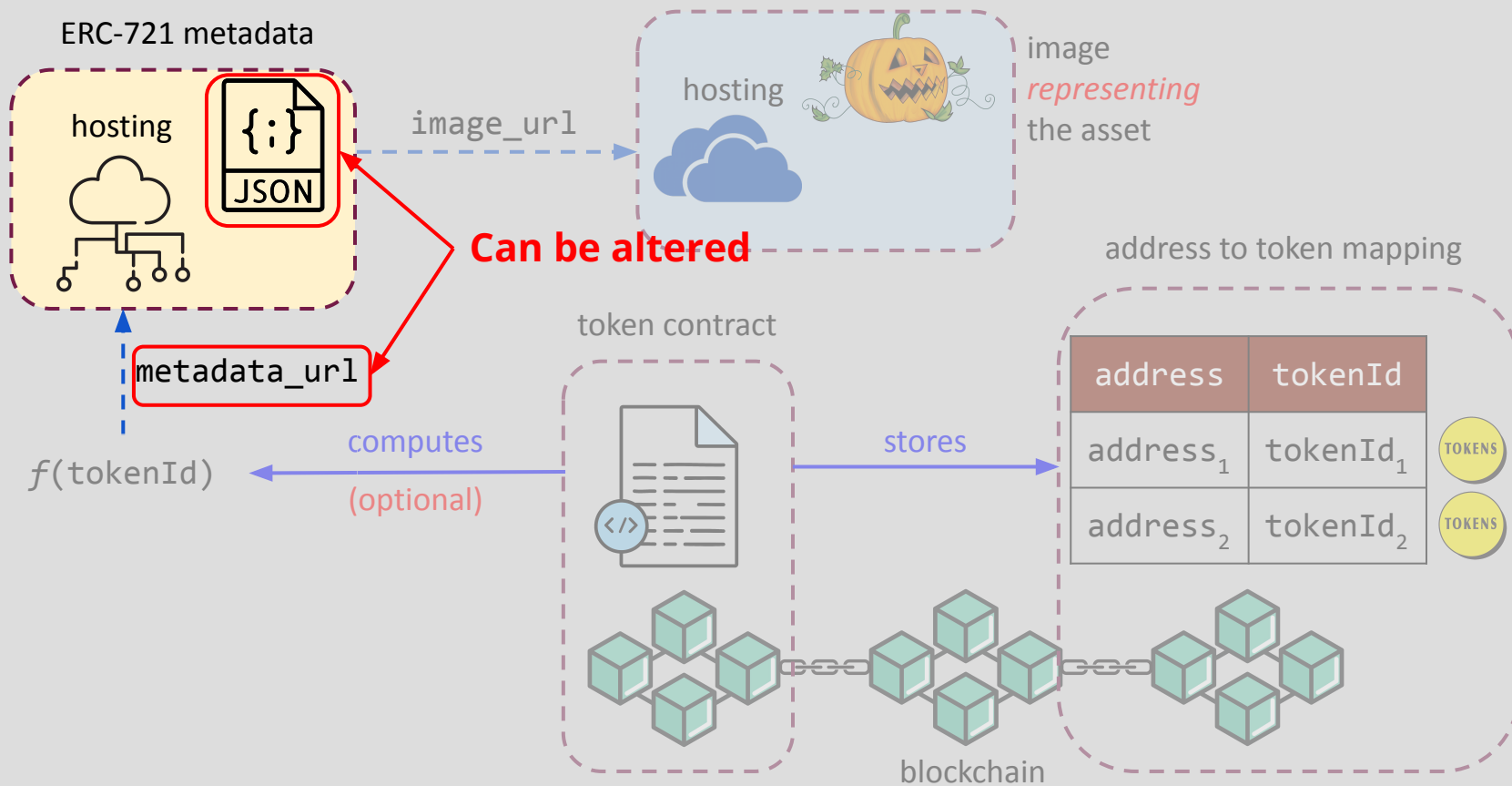
“Our analysis is ongoing, but our initial assessment indicates that the impact was limited, none of the impacted accounts had 2FA enabled” — Nifty Gateway team

Token minting→Verifiability of token contracts

- ★ A contract is 'verifiable', if
 - its source is submitted to Etherscan
 - Etherscan confirms a bytecode match
- ★ A malicious / malfunctioning token can
 - burn gas
 - not mint a token at all
 - mint more tokens than permitted by *rarity*



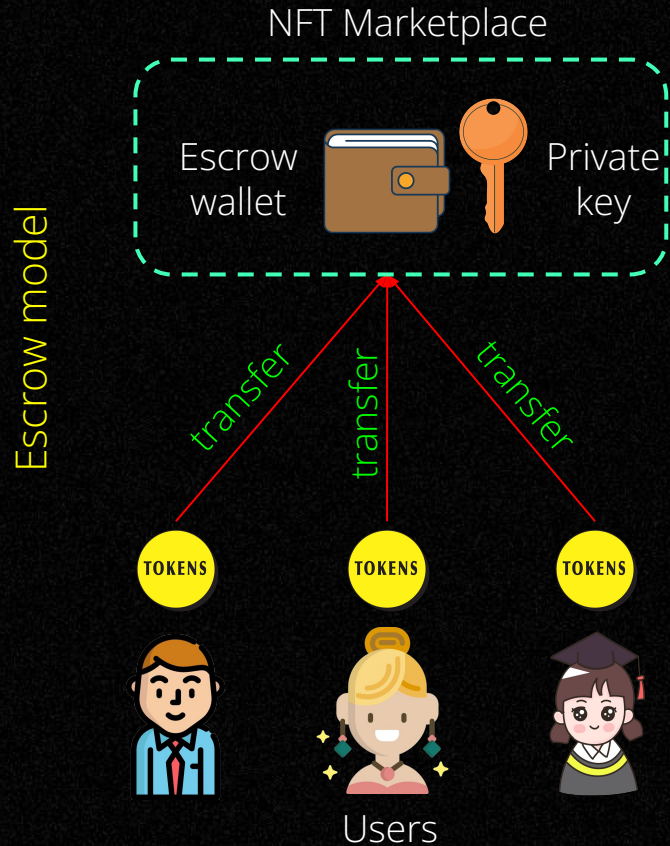
Token minting → Tampering with token metadata



Token minting→Tampering with token metadata

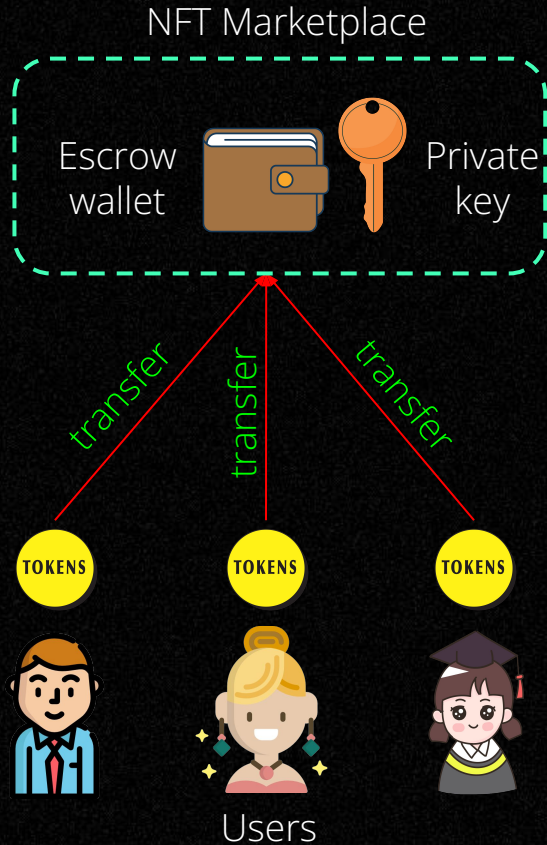


Token listing → Principle of least privilege

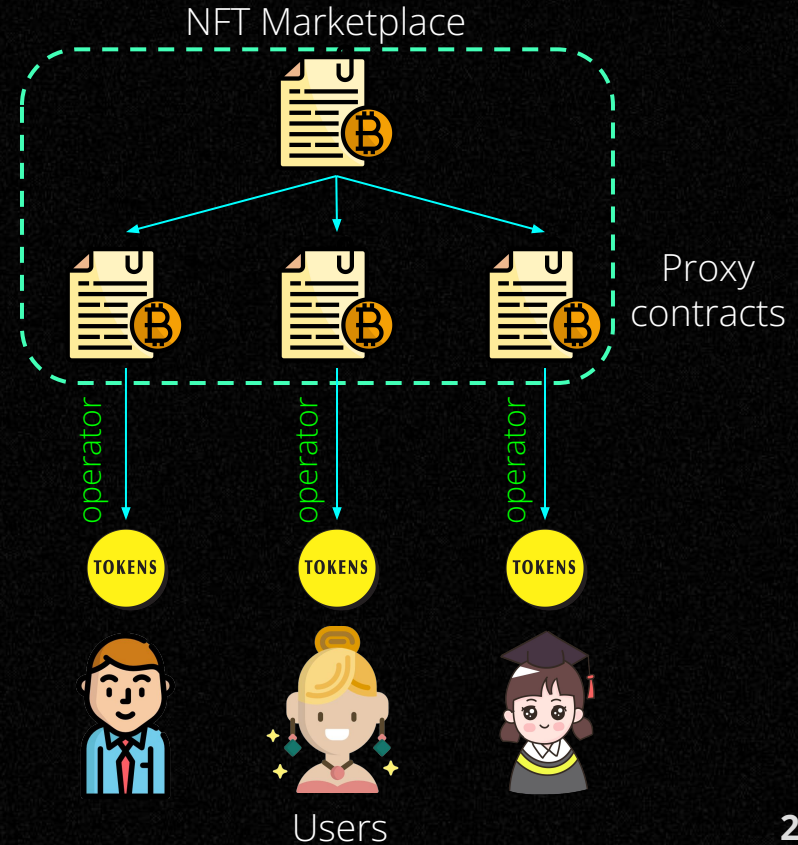


Token listing → Principle of least privilege

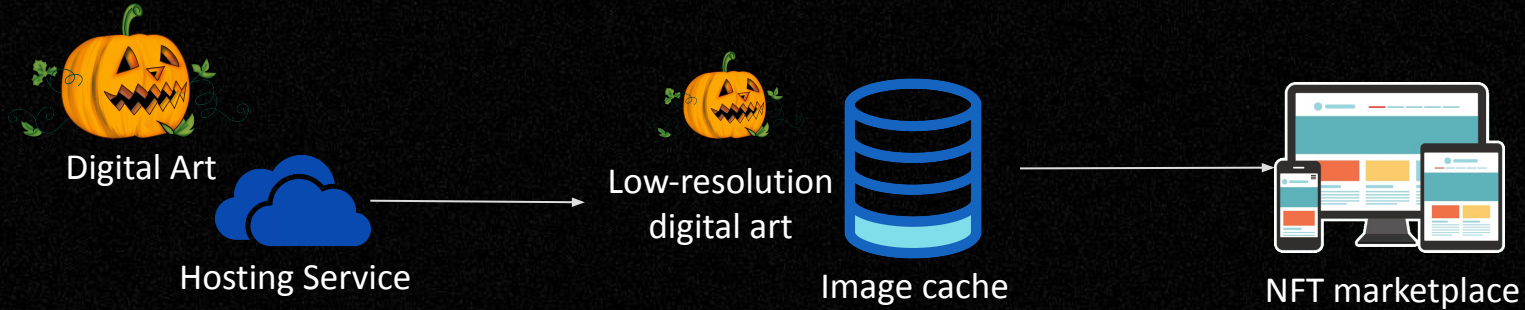
Escrow model



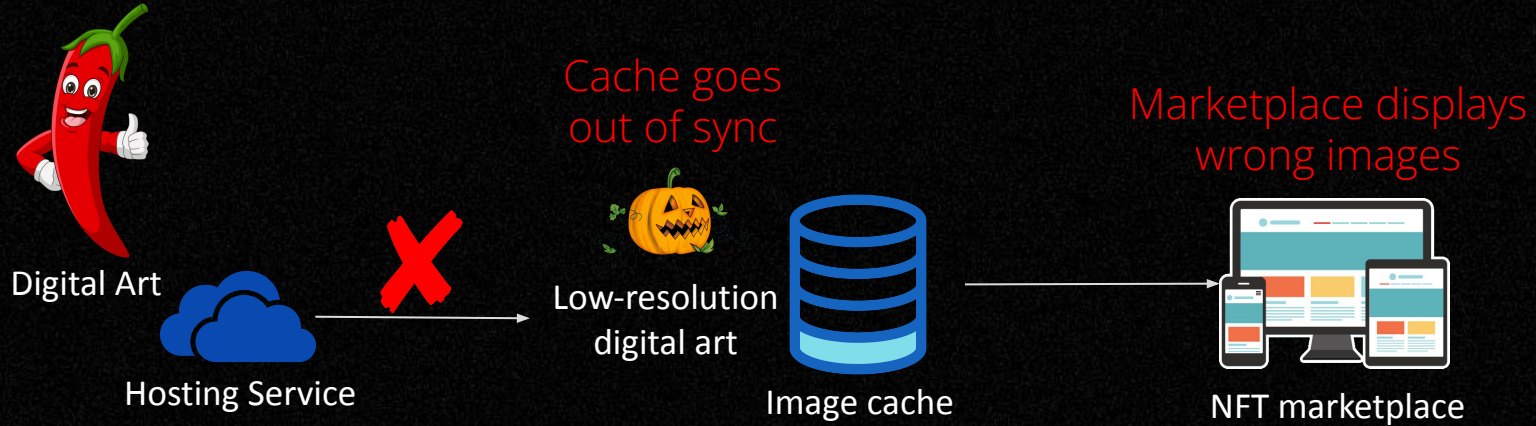
Operator model



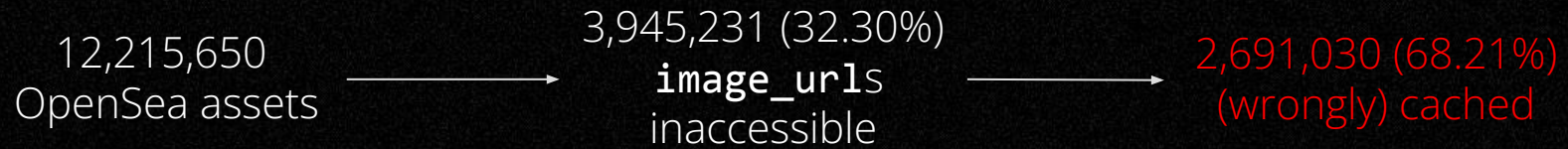
Token listing → Invalid caching



Token listing → Invalid caching



Token listing → Invalid caching



Token listing→Seller and collection verification

★ A verified seller / collection

- receives preferential treatment from the marketplace
- attracts greater attention of the buyer as they can shop with confidence

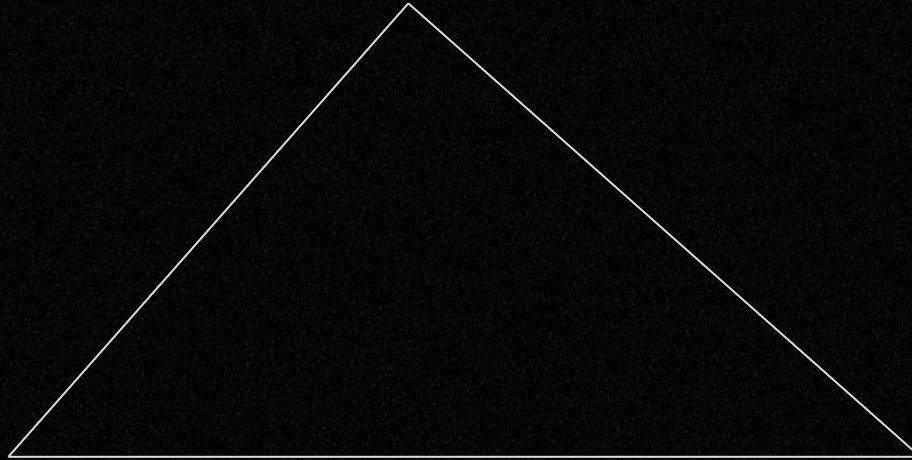
★ Typical verification requirements are

- **Seller**
 - sharing social media handles
 - sharing contact information
- **Collection**
 - collections needing to reach certain trading volume
 - submitting the draft files of the digital artworks

Token listing→Seller and collection verification

Verification badge overlaid on
profile pictures

Forging verification badge



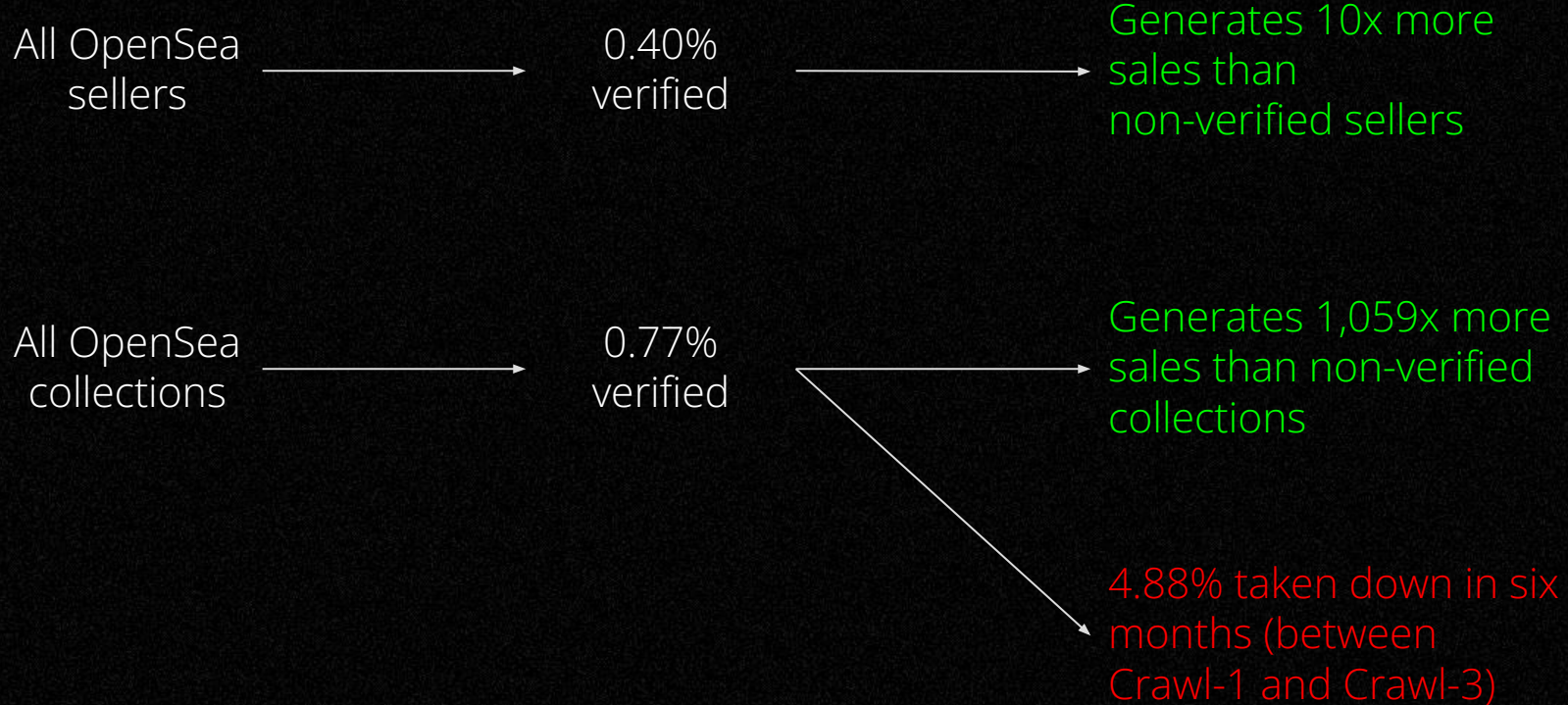
Impersonation

Submitting social media handles
without proving the ownership

Wash trading

Artificial trades to inflate the
trading volume

Token listing→Seller and collection verification

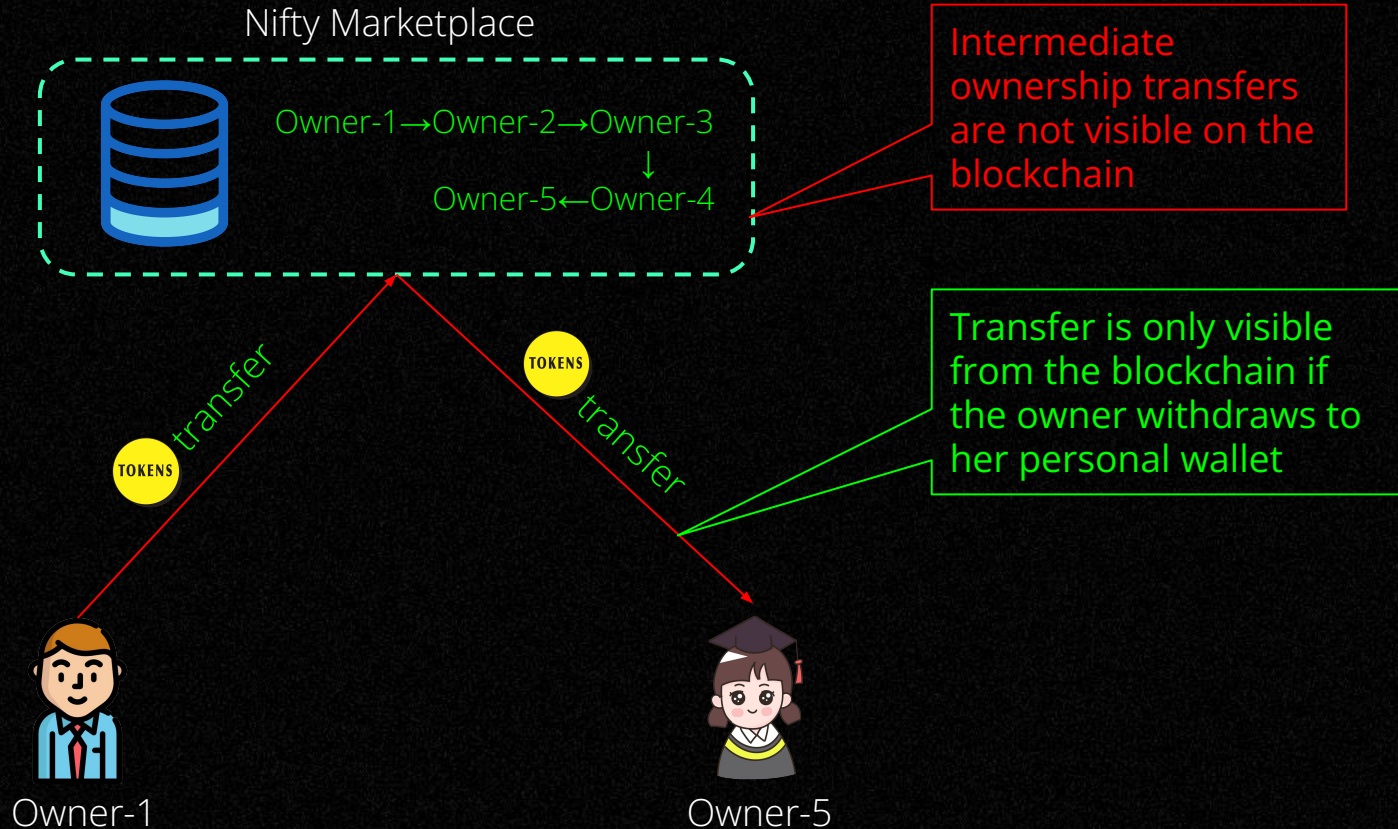


Token trading→Lack of transparency

- ★ NFT trades **should emit** sale / transfer events, which should include
 - address of the seller (current owner)
 - address of the buyer (new owner)
 - how much the NFT was sold for
 - time of ownership transfer

- ★ Sale / transfer events **should be stored** on-chain, because off-chain records are susceptible to
 - tampering
 - censorship
 - disappearance of NFT if the marketplace goes out of business
 - **NFT without decentralization—is that an “NFT” at all?**

Token listing → Lack of transparency



Token trading→Fairness in bidding

On-chain bidding

- ★ Bid appears on the blockchain
- ★ Bid amount has to be deposited while placing the bid

Off-chain bidding

- ★ Bid is recorded in an off-chain orderbook managed by the marketplace
- ★ Bid amount is deducted on execution

Token trading → Fairness in bidding

On-chain bidding

- ★ Bid appears on the blockchain
- ★ Bid amount has to be deposited while placing the bid

- ❑ Bid information is visible to the world
- ❑ Placing / cancelling bids costs gas, which prevents spurious bids

Off-chain bidding

- ★ Bid is recorded in an off-chain orderbook managed by the marketplace
- ★ Bid amount is deducted on execution

- ❑ Marketplace can inflate the bid volume to create hype
- ❑ Placing bid is inexpensive, which leads to large number of *casual bids*

Token trading → Fairness in bidding

	Total auctions	Auctions where highest bidder did not receive the item
OpenSea	48,862	16,215
Rarible	19,109	15,368

This is unfair, because the bid immediately below might be a lowball offer

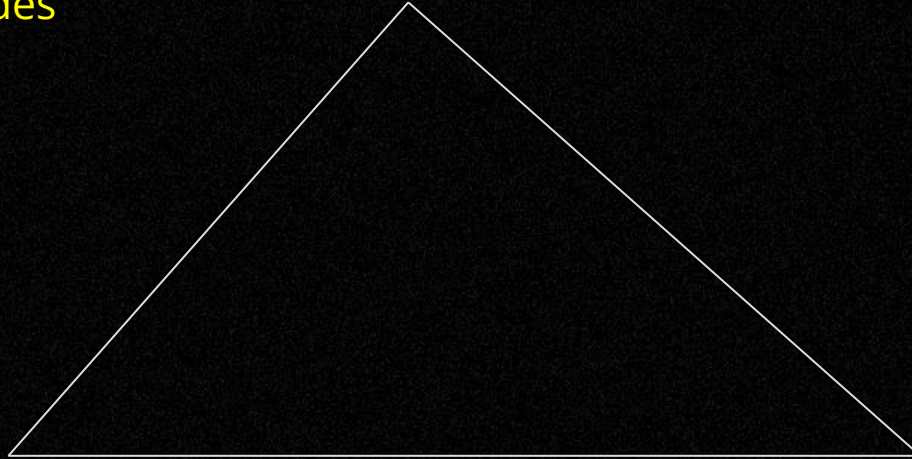
Token trading → Royalty and NFTM fee evasion



Royalty is the fee
earned by the creator
from secondary trades

Marketplaces store royalty
percentages off-chain

Cross-platform



Non-enforcement

Royalty is not enforced in the
token contract

Post-sales modification

A malicious creator can modify
royalty amount post primary sale

Token trading → Royalty and NFTM fee evasion

Non-enforcement



1. Asset listed in the marketplace
2. Difference between payment and transfer is at most 15 minutes

56,920 instances for assets listed in OpenSea

Token trading → Royalty and NFTM fee evasion

Post-sales modification

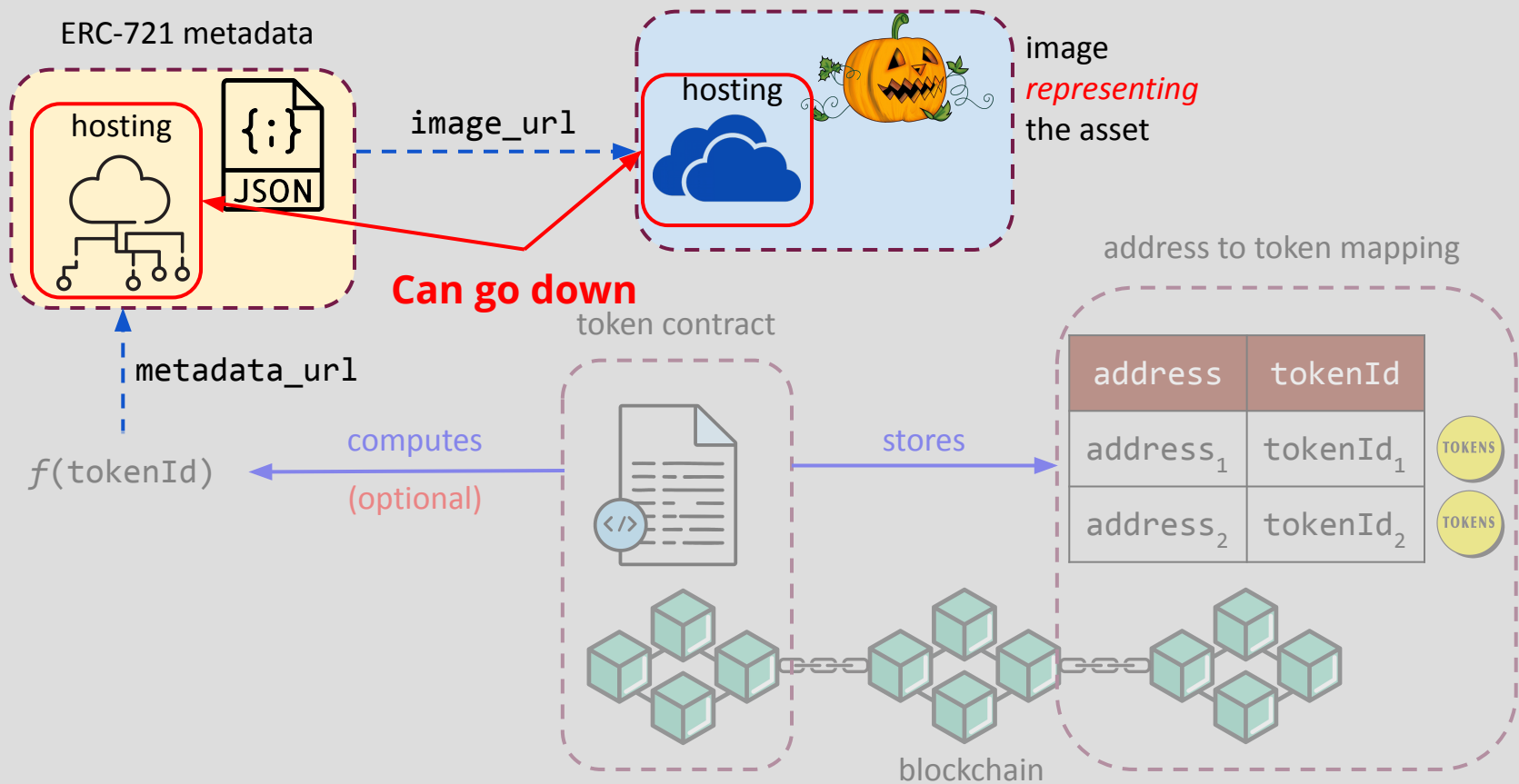


157,450 instances of royalty
modification in OpenSea



Issues with external entities

Disappearance of assets



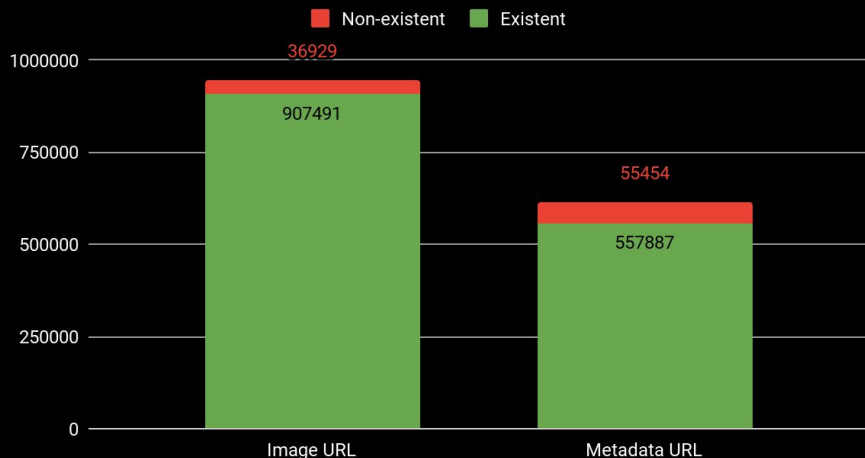
Disappearance of assets

- ★ NFTs hosted in IPFS are less likely to disappear, because
 - they can be self-hosted by the buyer (pinning)

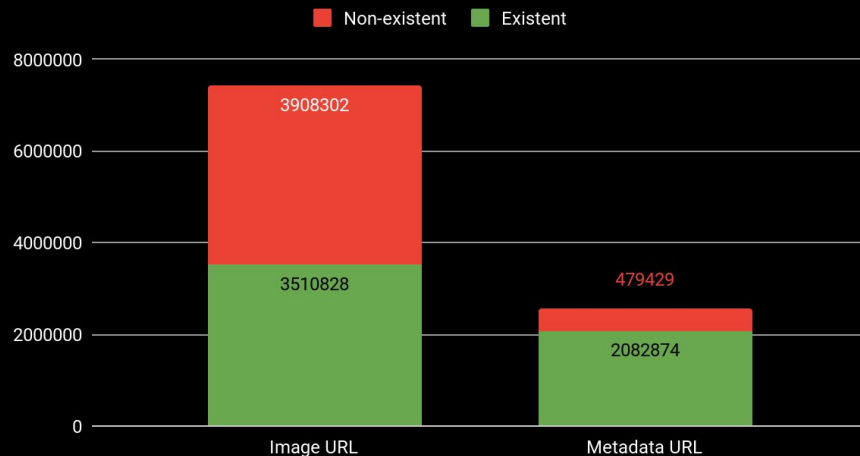
- ★ NFTs that store IPFS gateway URLs or hosted under web domains are problematic, because
 - the gateways or the web domains can go down

Disappearance of assets

IPFS URLs



Non-IPFS URLs



NFTs hosted in IPFS are less likely to disappear



Majority of the image URLs (88.71%) and metadata URLs (80.69%) are hosted on non-IPFS domains



Fraudulent user behaviors

Counterfeit NFT creation

Scammers create collections with names or visual appearances identical to the popular ones

★ Similar collection names

- fake collection name is a minor modification of a popular one, e.g., “CryptoSpells” vs. “CryptoSpells.”

★ Similar images

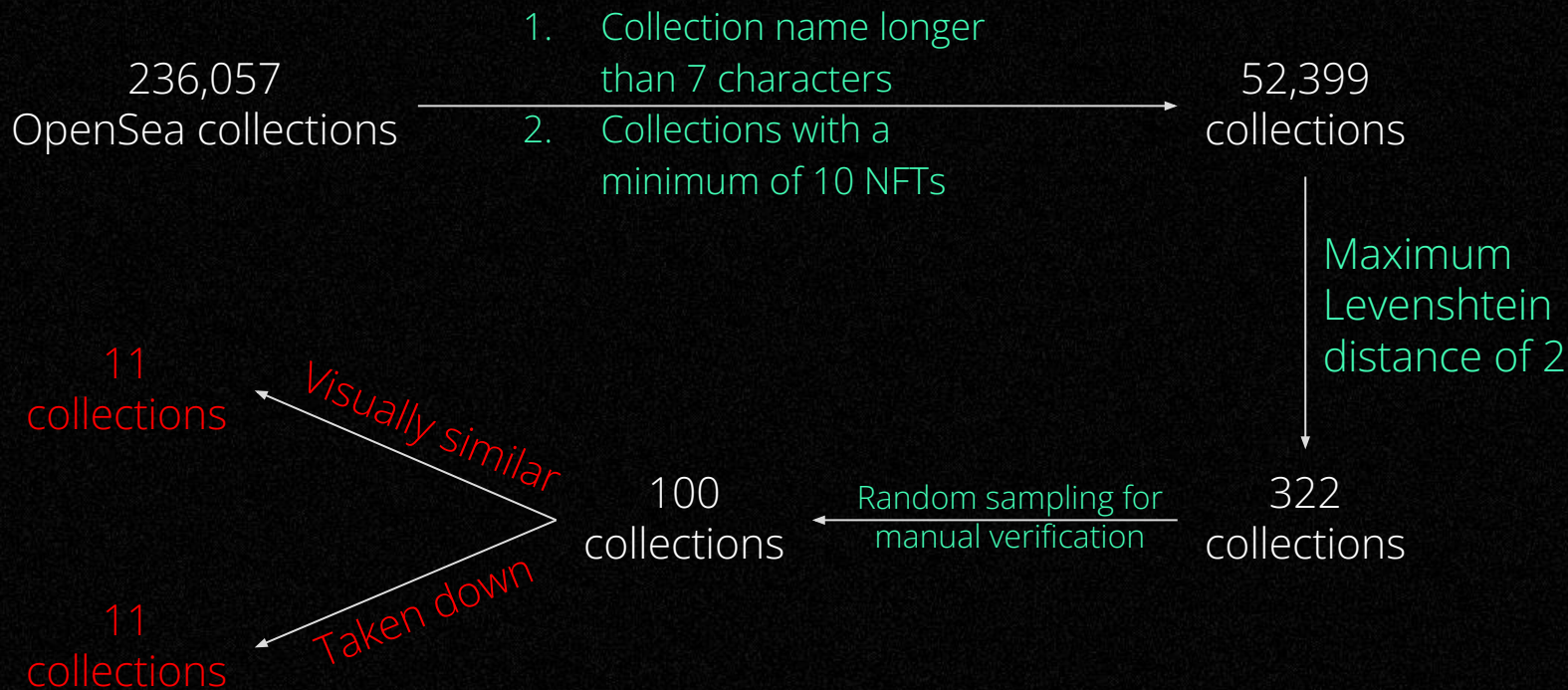
- copy the images pointed to by popular NFTs

★ Identical image URLs

- copy the **image_urls** of legitimate NFTs

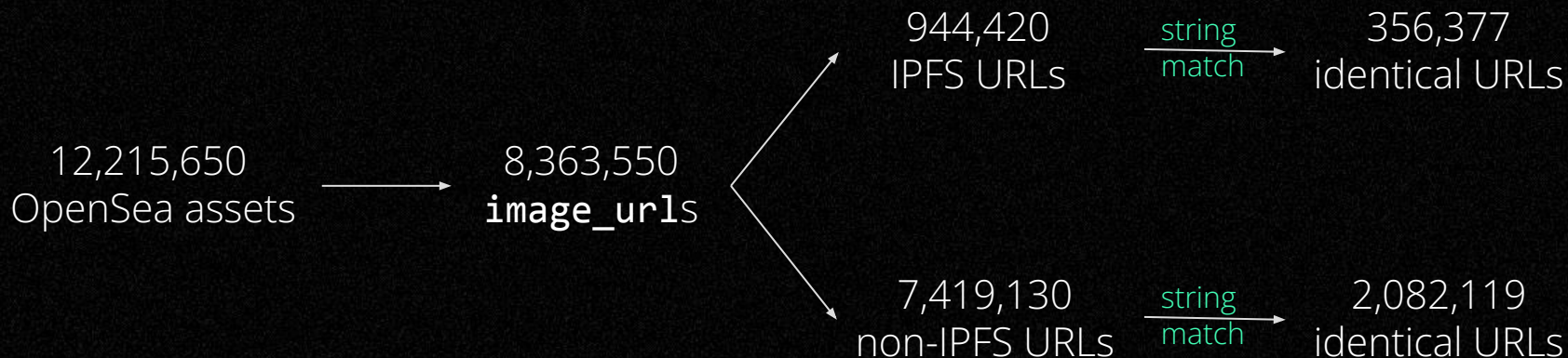
Counterfeit NFT creation

Similar collection names



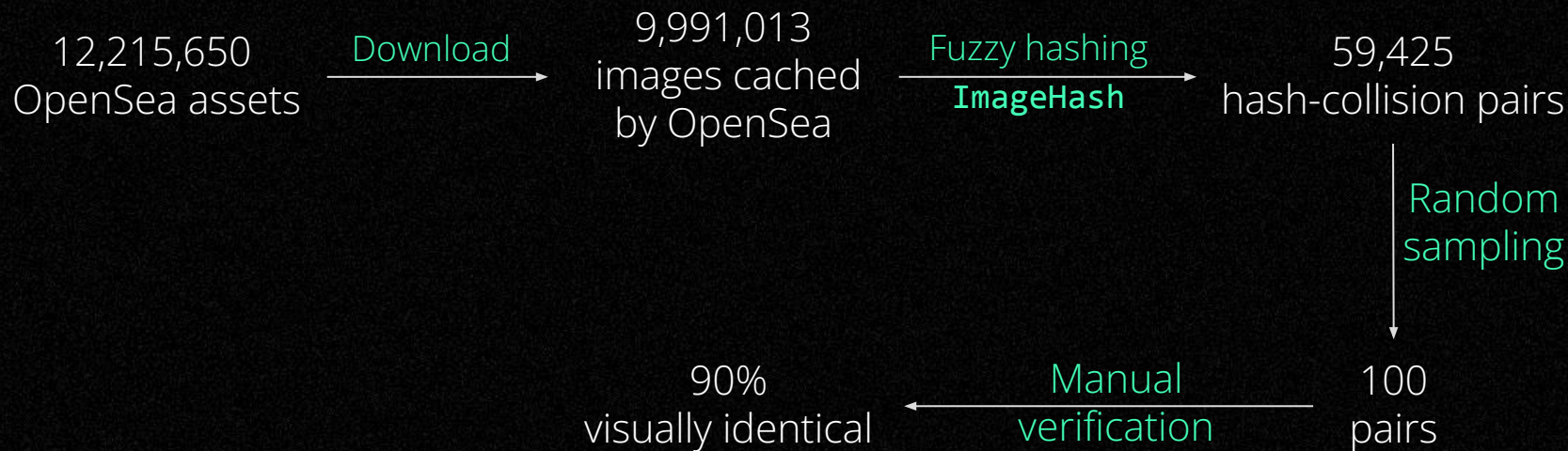
Counterfeit NFT creation

Identical image URLs



Counterfeit NFT creation

Similar images

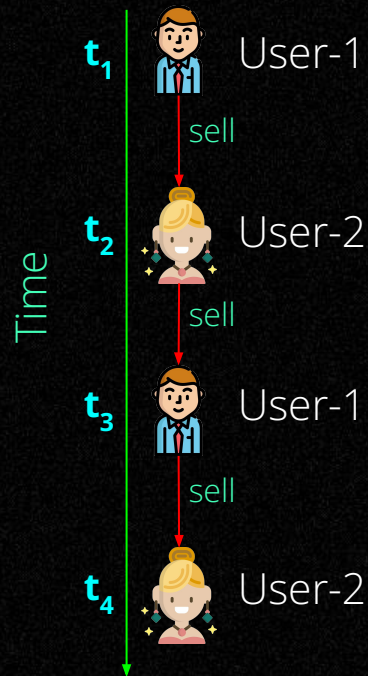


Trading Malpractices

- Trading malpractices involve (illegal?) market manipulation
- Following trading malpractices were measured on a dataset of 13,628,411 assets and 354,535,763 events collected from top 7 NFT marketplaces
 - Wash trading
 - Shill bidding
 - Bid shielding

Trading Malpractices→Wash trading

- ★ Artificially inflating the trading volume by generating “fake” trades to
 - create hype
 - satisfy marketplace verification condition
 - improve other metrics of financial interest



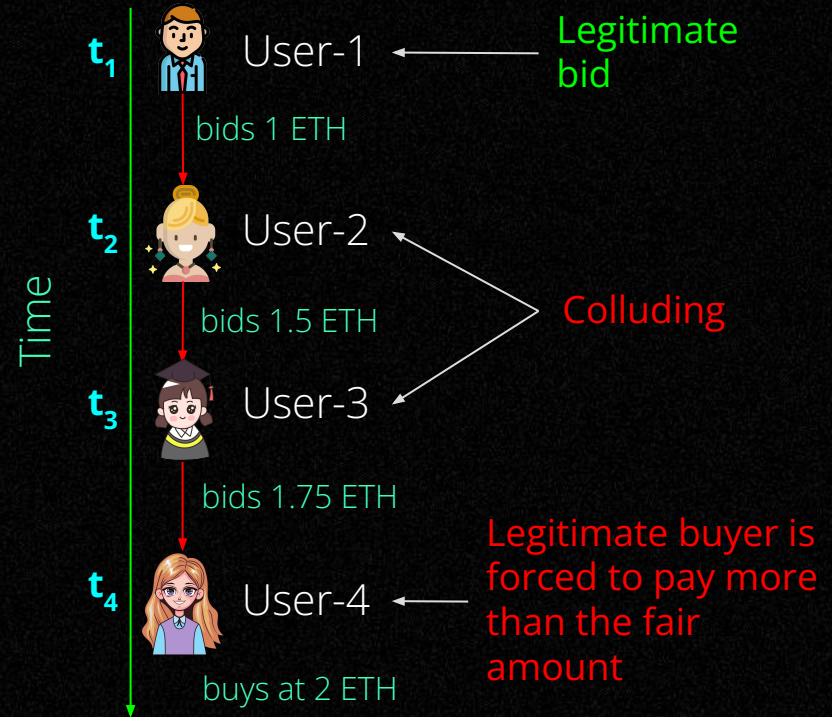
Trading Malpractices→Wash trading

9,393 instances of wash trading ————— \$96,858,093 USD in trading volume ————— 5,297 collections ————— 17,821 users

236,057 OpenSea collections ——— Trading volume over \$2K ———→ 8,869 collections ——— Wash trading is present ———→ 2,569 (28.97%) collections

Trading Malpractices → Shill bidding

- ★ Artificially inflating activity on an asset by placing “fake” bids to
 - create hype
 - bump up the price of an asset
- ★ Detecting shill bidding is difficult when looking at a single auction in isolation
 - we consider the simple case where a user repeatedly places bids in auctions, yet never (or rarely) purchases anything
- ★ $\text{shill profit} = \text{buy price} - \text{last legitimate bid}$

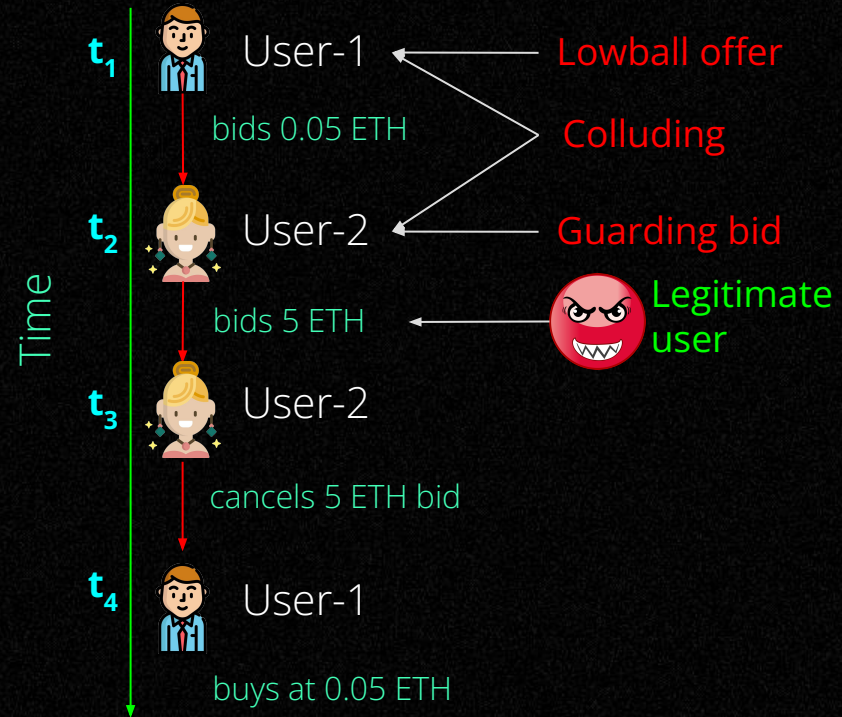


Trading Malpractices→Shill bidding



Trading Malpractices → Bid shielding

- ★ Guard a lowball offer with a high bid to deter legitimate buyers from placing bids
- ★ shielded bid difference = guarding bid amount - buy price



Trading Malpractices→Bid shielding



Conclusion

- ★ Systematic study of the NFT ecosystem
 - Identified three participating actors: marketplaces, external entities, users
 - Discovered security and privacy issues involving all three actors
- ★ Qualitative and quantitative analysis → Top 8 NFT marketplaces
 - Developed models to detect common trading malpractices
- ★ Many of the issues could potentially lead to financial losses

Image credits

- ★ <https://www.vecteezy.com>
- ★ <https://pixabay.com>
- ★ <https://www.freepik.com>