



## OECD International Academy for Tax Crime Investigation

*Anti-Money Laundering: Current Trends, Prosecutions,  
and the Challenges around Cryptocurrencies*



# NFTS, CRIME AND A BORED APE

# NFT Marketplaces

- A **web interface on a marketplace** is often used to assist users in buying and selling their NFTs.
- Market places mediate the sales transactions.



**OpenSea**

**SuperRare**



**RARIBLE**  
NFT Marketplace

# NFTs and “Crime”

- **Phishing & Theft**
  - Click on a link and get your wallet hacked
  - The hacker then transfers your NFT to their wallet
- **Scamming / Fraud / “Rug Pulls”**
  - Create a project
  - Mint and sell NFTs
  - Don’t build the promised project
  - Disappear with the money

# NFTs and Crime

- **Money laundering**
- **Wash trading**
- **Fraudulent fundraisers**

# Bored Ape #9410 Theft: What happened?

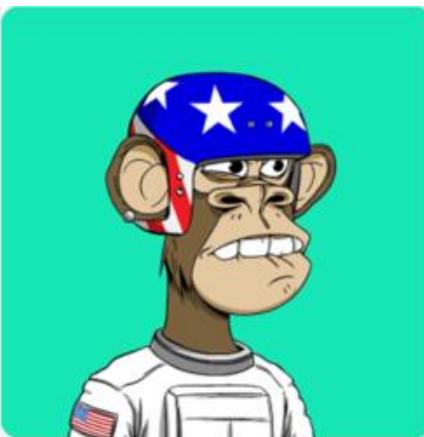
- A number of **Picasso's** Bored Apes and other NFTs were stolen on December 30, 2021.
- **Picasso** tweeted that he lost his collection through a **phishing scam** that gained access to his hot wallet after he clicked on a malicious link.



**'Lessons learned. Use a hardware wallet...'**

# Picasso's Stolen Apes, Mutants, and Clonex

- Ape 2771
- Ape 6416
- Ape 1623
- Ape 1708
- Ape 8214
- Ape 7528
- Ape 9988
- **Ape 9410**
- Mutant 25057
- Mutant 11177
- Mutant 28752
- Mutant 24718
- Mutant 2436
- Mutant 9278
- Mutant 2434
- Clonex 6801



# First Question:

## Can you freeze an Ape?



# Can you freeze Bored Ape NFTs?

- “OpenSea froze trading on the stolen items”
- You can ban NFT sales on a platform, but you can’t necessarily freeze the ability to sell the NFT.
- “Code is Law”: Some tokens are programmed so that they may be frozen, even burned.

## OpenSea freezes \$2.2M of stolen Bored Apes

Art gallery owner Todd Kramer had his valuable NFT collection stolen from his hot wallet yesterday, so OpenSea froze the stolen assets worth about \$2.2 million.



# OpenSea & Freezing

**“We do not have the power to freeze or delist NFTs that exist on these blockchains, however we do disable the ability to use OpenSea to buy or sell stolen items.”**

“It’s an article of faith that crypto transactions are irreversible. But there’s nothing inherent in blockchain technology that requires that, and some crypto projects already allow reversals.”



**OpenSea**

# OpenSea (<https://opensea.io/>)

- NFT Trading Platform
- “The world’s first and largest NFT Marketplace.”
- Founded in 2017
- Over \$2.7 Billion in revenue in 2021.
- Reports indicate that several million dollars of NFTs have been stolen from OpenSea.
- Law Enforcement friendly.

# Each NFT has an Information page

The image shows a screenshot of an NFT information page on OpenSea. The NFT is a Bored Ape Yacht Club #9410, featuring a cartoon monkey wearing a blue and red baseball cap with stars. A red arrow points to the image with the label "NFT Image". The page includes the project name "Bored Ape Yacht Club" and the creator "BoredApeYachtClub". A red arrow points to this information with the label "NFT Project/Creator". The page also displays the highest offer at 100.1 (worth \$303,977.67) and a "Make offer" button. A red arrow points to the price history chart with the label "Price History". The chart shows the price increasing over time, with a significant jump around January 4th. The page also includes a "Description" section and a "Created by" note.

**NFT Image**

**NFT Project/Creator**

**Price History**

Bored Ape Yacht Club

#9410

Owned by CapetainTrippyVault 63 favorites

Highest offer

100.1 (\$303,977.67)

Make offer

Price History

All Time Avg. Price \$55.038

Description

Created by BoredApeYachtClub

<https://opensea.io/assets/0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d/9410>

Filter

Sales X

Transfers X

Detailed Sales  
and Transfer  
History

Event	Price	From	To	Date
Transfer		C310E7	0x0888_Capital	3 months ago 
Transfer		0x0888_Capital	C310E7	3 months ago 
Sale	82	3DD59D 	0x0888_Capital	3 months ago 
Transfer		3DD59D 	0x0888_Capital	3 months ago 
Transfer		Picasso	3DD59D 	3 months ago 

Sale	82	3DD59D 	This account may be compromised
Transfer		3DD59D 	0x0888_Capital
Transfer		Picasso	3DD59D 

Theft  
transaction

# NFT Information: The Theft

- Note that it was a “Transfer”

 Sale	♦ 82	3DD59D 	0x0888_Capital	3 months ago 
 Transfer		3DD59D 	0x0888_Capital	
 Transfer		Picasso	3DD59D 	3 months ago 

Date and Time of Transfer/Theft

December 30 2021, 6:06 am

Link to the transaction on Etherscan Blockchain Explorer



# Rapid sale after theft

## Stolen from Picasso

Transfer

3DD59D !

0x0888\_Capital

December 30 2021, 6:06 am

Transfer

Picasso

3DD59D !

3 months ago

## Quickly sold to 0x0888\_Capital for 82 ETH

Transfer

0x0888\_Capital

C310E7

December 30 2021, 7:08 am

Sale

82

3DD59D !

0x0888\_Capital

3 months ago

Transfer

3DD59D !

0x0888\_Capital

3 months ago



# Theft transaction (Bored Ape #9410) OpenSea links to Etherscan

The screenshot shows a web browser with two tabs open. The top tab is on the OpenSea website, displaying a Bored Ape NFT (Bored Ape #9410) with a sale history. The bottom tab is on the Etherscan website, showing the transaction details for the same NFT. A large red arrow points from the OpenSea page to the Etherscan page, highlighting the connection between the two platforms.

opensea.io/assets/0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d/9410

Search items, collections, and accounts

Explore Stats Resources

Sale 82 3DD59D ! 0x0888\_Capital 4 months ago

Transfer 3DD59D ! 0x0888\_Capital December 30 2021, 6:06 am

Transfer Picasso 3DD59D ! 4 months ago

OpenSea Links to Etherscan

etherscan.io/tx/0xb9defcdd0d07c4c931c406a210d924eb7f3d437b7fdb7f5b6afa1742694184a

Etherscan All Filters

Eth: \$3,147.48 (+2.54%) | 102 Gwei

<https://etherscan.io/tx/0xb9defcdd0d07c4c931c406a210d924eb7f3d437b7fdb7f5b6afa1742694184a>

## Theft transaction details

Transaction Details < > Buy

Overview Logs (2) State Comments

⑦ Transaction Hash: 0xb9defcdd0d07c4c931c406a210d924eb7f3d437b7fdb...  
⑦ Status: Success  
⑦ Block: 13905012 724102 Block Confirmations  
⑦ Timestamp: 112 days 9 hrs ago (Dec-30-2021 06:06:16) Confirmed within 30s  
⑦ Transaction Action: Transfer of BoredApeYach... (BAYC) From 0x9e437b064fc... To 0x3dd59de66e2ad31a7d...  
1 of Token ID [9410]  
From: toddkramer.eth  
Interacted With (To): Contract 0xbc4ca0eda7647a8ab7c2061c2e118a... (Bored Ape Yacht Club: BAYC Token) ✓  
From 0x9e437b064fc... To Fake\_Phishing5... For ERC-721 Token ID [9410] BoredApeYach... (BAYC)  
BoredApeYach... (BAYC)

From 0x9e437b064fc... (Picasso)

To 0x3dd59de66e2ad31a7d... (Thief)

Token #9410

Transaction mediated by the Bored Ape Yacht Club smart contract

<https://etherscan.io/tx/0xb9defcdd0d07c4c931c406a210d924eb7f3d437b7fdbc7f5b6afa1742694184a>

# EtherScan: Tokens can be looked up

- **URL:**

**Token creation contract + token numeric identifier:**

<https://etherscan.io/token/contract?a=ID>

<https://etherscan.io/nft/contract/ID>

- **Bored Ape #9410**

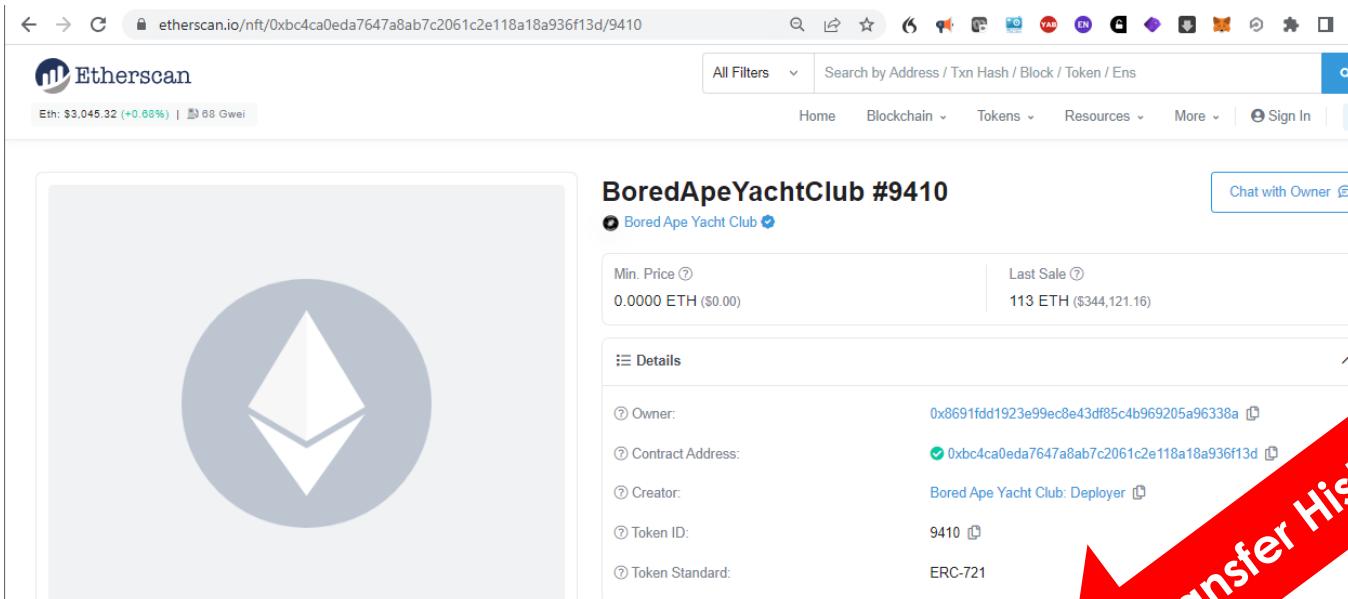
- Contract#: 0xBC4CA0EdA7647A8aB7C2061c2E118A18a936f13D
- Ape#: 9410

<https://etherscan.io/token/0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d?a=9410>

<https://etherscan.io/nft/0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d/9410>

# Token (Bored Ape #9410)

<https://etherscan.io/nft/0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d/9410>



Etherscan

Eth: \$3,045.32 (+0.68%) | 68 Gwei

Min. Price ⑦ 0.0000 ETH (\$0.00) Last Sale ⑦ 113 ETH (\$344,121.16)

Details

Owner: 0x8691fdd1923e99ec8e43df85c4b969205a96338a

Contract Address: 0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d

Creator: Bored Ape Yacht Club: Deployer

Token ID: 9410

Token Standard: ERC-721

Chat with Owner

BoredApeYachtClub #9410

Bored Ape Yacht Club

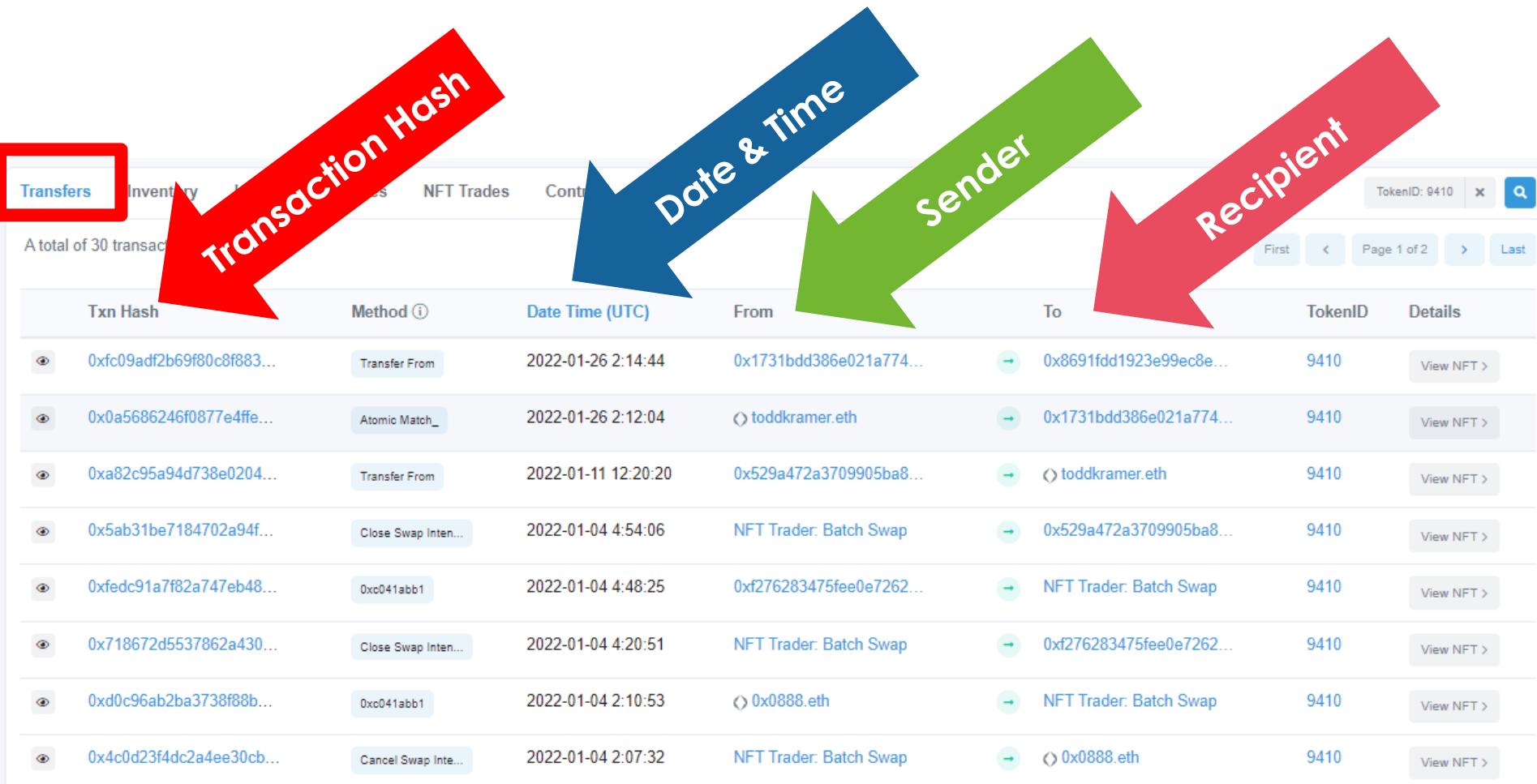
Item Activity

A total of 30 records found

Txn Hash	Date Time (UTC)	Action	Price	From	To
0xfc09adf2b69f80c8f883...	2022-01-26 2:14:44	Transfer		0x1731bdd386e021a774...	0x8691fdd1923e99ec8e...
0x0a5686246f0877e4ffe...	2022-01-26 2:12:04	Sale	169.69 ETH (\$516,760.35)	0x9e437b064fcf780180...	0x1731bdd386e021a774...
0xa82c95a94d738e0204...	2022-01-11 12:20:20	Transfer		0x529a472a3709905ba8...	0x9e437b064fcf780180...
0x5ab31be7184702a94f...	2022-01-04 4:54:06	Transfer		0xc310e760778ecbca4c...	0x529a472a3709905ba8...
0xfedc91a7f82a747eb48...	2022-01-04 4:48:25	Transfer		0xf276283475fee0e7262...	0xc310e760778ecbca4c...
0x718672d5537862a430...	2022-01-04 4:20:51	Transfer		0xc310e760778ecbca4c...	0xf276283475fee0e7262...
0xd0c96ab2ba3738f88b...	2022-01-04 2:10:53	Transfer		0xc2a59d94b69f7739f77...	0xc310e760778ecbca4c...

Transfer History

# Transfer History (Bored Ape #9410)



Transfers Inventory NFTs NFT Trades Contracts

A total of 30 transactions

First < Page 1 of 2 > Last

Txn Hash	Method	Date Time (UTC)	From	To	TokenID	Details
0xfc09adf2b69f80c8f883...	Transfer From	2022-01-26 2:14:44	0x1731bdd386e021a774...	0x8691fdd1923e99ec8e...	9410	<a href="#">View NFT &gt;</a>
0xa5686246f0877e4ffe...	Atomic Match...	2022-01-26 2:12:04	0x1731bdd386e021a774...	0x1731bdd386e021a774...	9410	<a href="#">View NFT &gt;</a>
0xa82c95a94d738e0204...	Transfer From	2022-01-11 12:20:20	0x529a472a3709905ba8...	0x1731bdd386e021a774...	9410	<a href="#">View NFT &gt;</a>
0x5ab31be7184702a94f...	Close Swap Inten...	2022-01-04 4:54:06	NFT Trader: Batch Swap	0x529a472a3709905ba8...	9410	<a href="#">View NFT &gt;</a>
0xfedc91a7f82a747eb48...	0xc041abb1	2022-01-04 4:48:25	0xf276283475fee0e7262...	NFT Trader: Batch Swap	9410	<a href="#">View NFT &gt;</a>
0x718672d5537862a430...	Close Swap Inten...	2022-01-04 4:20:51	NFT Trader: Batch Swap	0xf276283475fee0e7262...	9410	<a href="#">View NFT &gt;</a>
0xd0c96ab2ba3738f88b...	0xc041abb1	2022-01-04 2:10:53	0x0888.eth	NFT Trader: Batch Swap	9410	<a href="#">View NFT &gt;</a>
0x4c0d23f4dc2a4ee30cb...	Cancel Swap Inten...	2022-01-04 2:07:32	NFT Trader: Batch Swap	0x0888.eth	9410	<a href="#">View NFT &gt;</a>

# Thief's Address (0x3dd59d...)

## 39 transactions

Transactions	Internal Txns	Erc20 Token Txns	Erc721 Token Txns	Analytics	Comments
Latest 25 from a total of 39 transactions					
Txn Hash	Method ⓘ	Block ↴	Date Time (UTC) ↴	From ↴	To ↴
<a href="#">0x91911b441021ba5498...</a>	Transfer	13905971	2021-12-30 9:55:19	Fake_Phishing5028	OUT <a href="#">0x0c4699dc0d169a8f01...</a>
<a href="#">0x8d058bf03ca4c2cdb0c...</a>	Safe Transfer Fr...	13905788	2021-12-30 9:08:07	Fake_Phishing5028	OUT <a href="#">Bored Ape Yacht Club: B...</a> 0 Ether
<a href="#">0xae14a1d1bbb58300cd...</a>	Safe Transfer Fr...	13905774	2021-12-30 9:05:46	Fake_Phishing5028	OUT <a href="#">Bored Ape Yacht Club: B...</a> 0 Ether
<a href="#">0x60b8344dffcbd186e6b...</a>	Safe Transfer Fr...	13905763	2021-12-30 9:04:23	Fake_Phishing5028	OUT <a href="#">Bored Ape Yacht Club: B...</a> 0 Ether
<a href="#">0xd04cdbf4ff97aaea265...</a>	Safe Transfer Fr...	13905759	2021-12-30 9:02:26	Fake_Phishing5028	OUT <a href="#">Bored Ape Yacht Club: B...</a> 0 Ether
<a href="#">0x8dd950b4b568b1a6b2...</a>	Safe Transfer Fr...	13905759	2021-12-30 9:02:26	Fake_Phishing5028	OUT <a href="#">Bored Ape Yacht Club: B...</a> 0 Ether
<a href="#">0xf7e7d8a534c6805df41...</a>	Withdraw	13905335	2021-12-30 7:27:52	Fake_Phishing5028	OUT <a href="#">Wrapped Ether</a> 0 Ether
<a href="#">0xa24c78f7993240b883...</a>	Atomic Match_	13905318	2021-12-30 7:24:02	Fake_Phishing5028	OUT <a href="#">OpenSea: Wyvern Exch...</a> 0 Ether
<a href="#">0x07bba6b50b70a86ad2...</a>	Atomic Match_	13905312	2021-12-30 7:23:04	Fake_Phishing5028	OUT <a href="#">OpenSea: Wyvern Exch...</a> 0 Ether
<a href="#">0x614b63672842d5e59e...</a>	Atomic Match_	13905311	2021-12-30 7:22:11	Fake_Phishing5028	OUT <a href="#">OpenSea: Wyvern Exch...</a> 0 Ether
<a href="#">0x5b1df3bdc015d8a0e1...</a>	Atomic Match_	13905307	2021-12-30 7:21:34	Fake_Phishing5028	OUT <a href="#">OpenSea: Wyvern Exch...</a> 0 Ether
<a href="#">0xe97920db2c85ea2fa2...</a>	Atomic Match_	13905307	2021-12-30 7:21:34	Fake_Phishing5028	OUT <a href="#">OpenSea: Wyvern Exch...</a> 0 Ether

# Thief's transaction activity

- **Token Contracts**
  - Bored Ape Yacht Club
  - Mutant Ape Yacht Club
  - Clone X Token
  - Wrapped Ether contract
- **Platforms**
  - OpenSea / Wyvern
  - Tornado Cash (Mixer)
- **Addresses:**
  - 0x0c4699dc0d169a8f015351db285f48256690f0e9
  - 0xf76179bb0924ba7da8e7b7fc2779495d7a7939d8
  - 0x23bc98b530BDF1b2471350159e2C3bb507d8eAFD



Etherscan

Eth: \$3,116.45 (+1.53%) | 76 Gwei

Transactions

For 0x3dd59de66e2ad31a7d663df977ddd6e5f2a5f6b6

Public Name Tag (viewable by anyone)

Fake\_Phishing5028

# Token transfers cost ETH, but have a 0 ETH transfer value

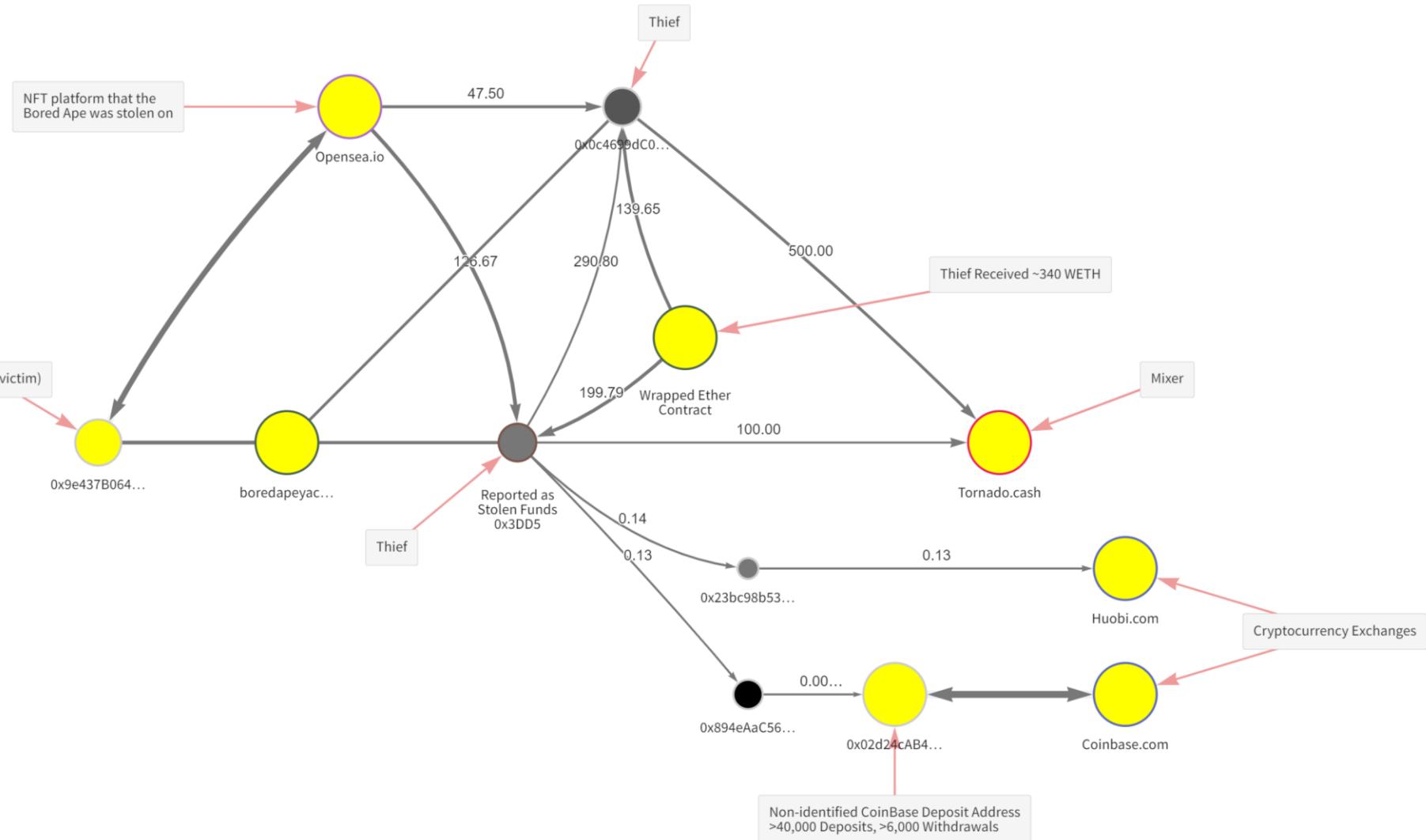
- Following the money is different than following the tokens.
- You need to do both to have a full picture.

From	To	Value	Txn Fee
Fake_Phishing5028	0x0c4699dc0d169a8f01...	290.798404812147437 Ether	0.0023331615 ⚡
Fake_Phishing5028	0x0c4699dc0d169a8f01...	0 Ether	0.007619063486 ⚡
Fake_Phishing5028	0x0c4699dc0d169a8f01...	0 Ether	0.007909471999 ⚡
Fake_Phishing5028	0x0c4699dc0d169a8f01...	0 Ether	0.01219324952 ⚡



**Follow the Money & Follow the Tokens**

# The Big Picture (NFTs, ETH, Smart Contracts)



# Theft Transaction

- OpenSea gives the date and time of the theft transaction
- OpenSea links to Etherscan Transaction

Transfer	3DD59D !	0x0888_Capital	December 30 2021, 6:06 am
Transfer	Picasso	3DD59D !	4 months ago 

- Find the transaction in Chainalysis using:
  - The transaction hash of the theft as found in Etherscan.
  - Using the date and time of the transaction to narrow in on the theft transaction.

# Theft Transaction: Dec 30, 6:06

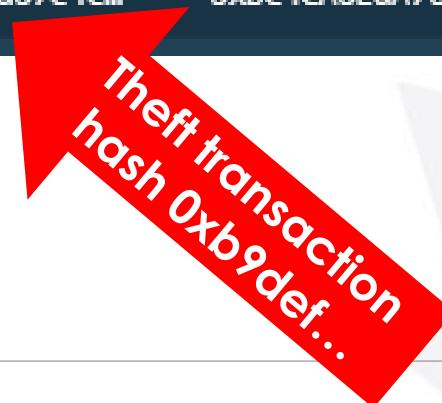
- 0xb9defcdd0d07c4c931c406a210d924eb7f3d437b7fdb7f5b6afa1742694184a



# Theft Transaction: Dec 30, 6:06

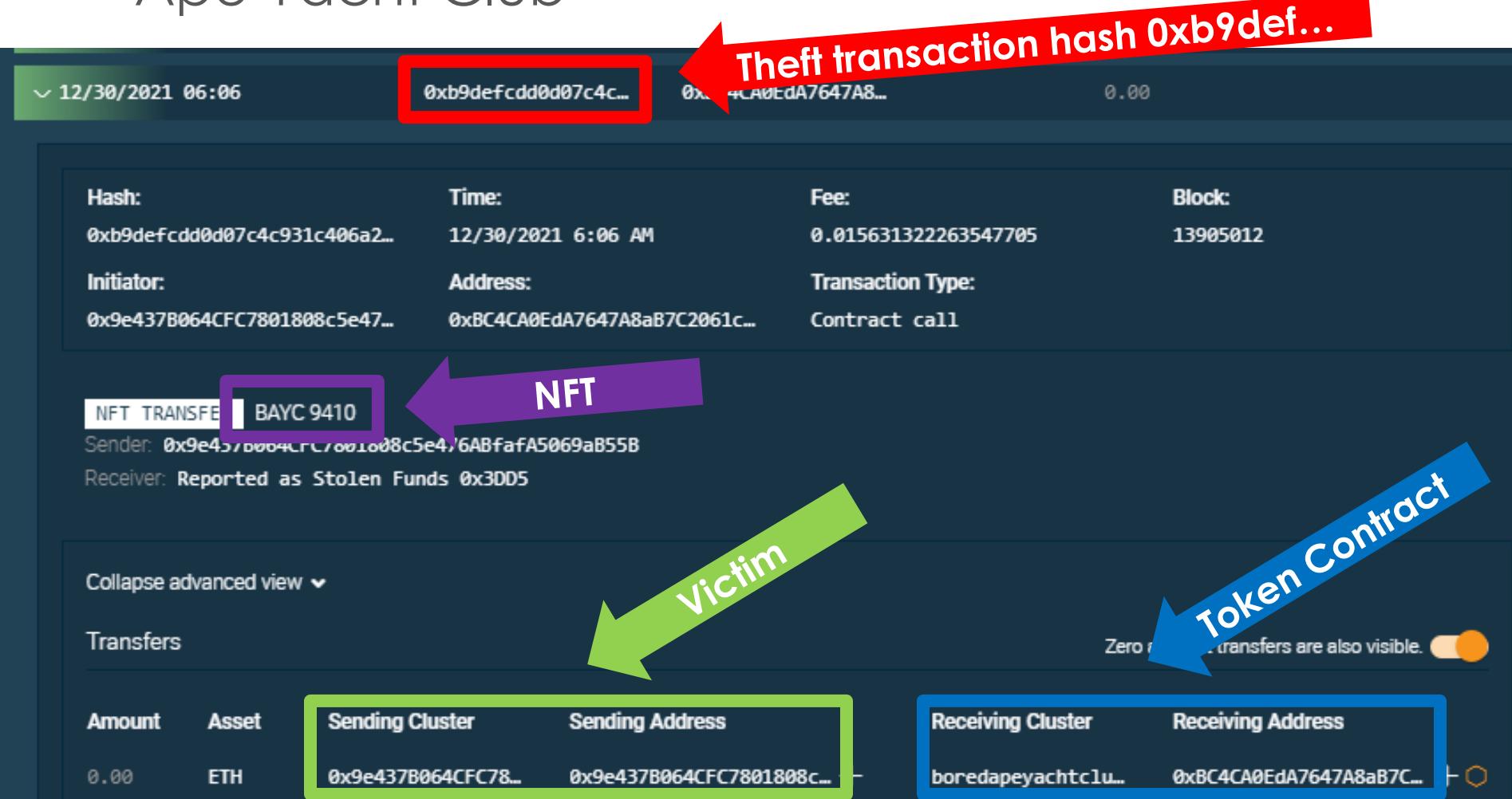
- Three transactions took place on Dec 30 at 6:06 AM.
- Three apes were stolen at the same time

> 12/30/2021 06:06	0xdadd1f51ad5addc...	0xBC4CA0EdA7647A8...	0.00
> 12/30/2021 06:06	0x906ac4cab171be1...	0xBC4CA0EdA7647A8...	0.00
> 12/30/2021 06:06	0xb9defcdd0d07c4c...	0xBC4CA0EdA7647A8...	0.00



# Theft of Bored Ape 9410

- Note that the receiving address is the Bored Ape Yacht Club



Theft transaction hash 0xb9def...

12/30/2021 06:06

0xb9defcdd0d07c4c...

0x9e437b064cfc7801808c5e47...

0.00

Hash: 0xb9defcdd0d07c4c931c406a2... Time: 12/30/2021 6:06 AM Fee: 0.015631322263547705 Block: 13905012

Initiator: 0x9e437b064cfc7801808c5e47... Address: 0xBC4CA0EdA7647A8aB7C2061c... Transaction Type: Contract call

NFT TRANSFER | BAYC 9410

Sender: 0x9e437b064cfc7801808c5e47.../6ABfafA5069aB55B

Receiver: Reported as Stolen Funds 0x30D5

Collapse advanced view ▾

Transfers

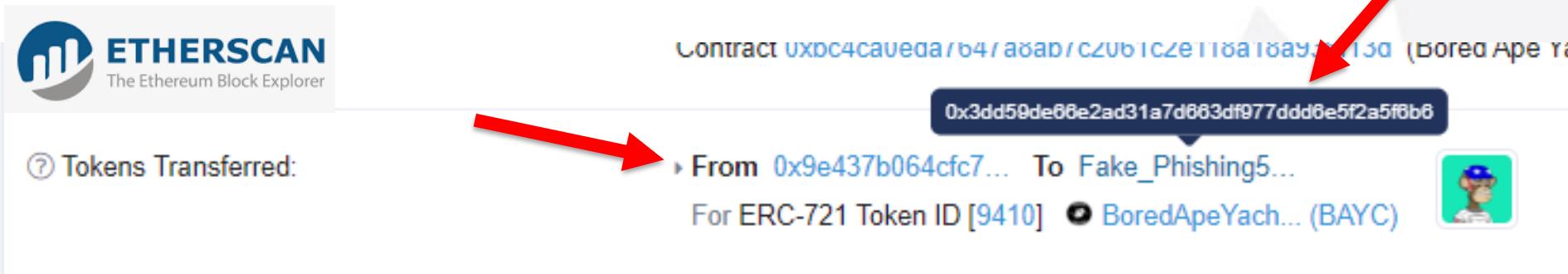
Amount Asset Sending Cluster Sending Address Receiving Cluster Receiving Address

0.00 ETH 0x9e437b064cfc7801808c5e47... 0x9e437b064cfc7801808c5e47.../boredapeyachtclu... 0xBC4CA0EdA7647A8aB7C2061c...

Zero value transfers are also visible.

# Look to Etherscan to identify the token recipient

- Use the theft **Transaction ID**
- Look at the **Tokens Transferred** information
- Find the recipient's address
- **Enter the thief's address into Chainalysis**



ETHERSCAN  
The Ethereum Block Explorer

Tokens Transferred:

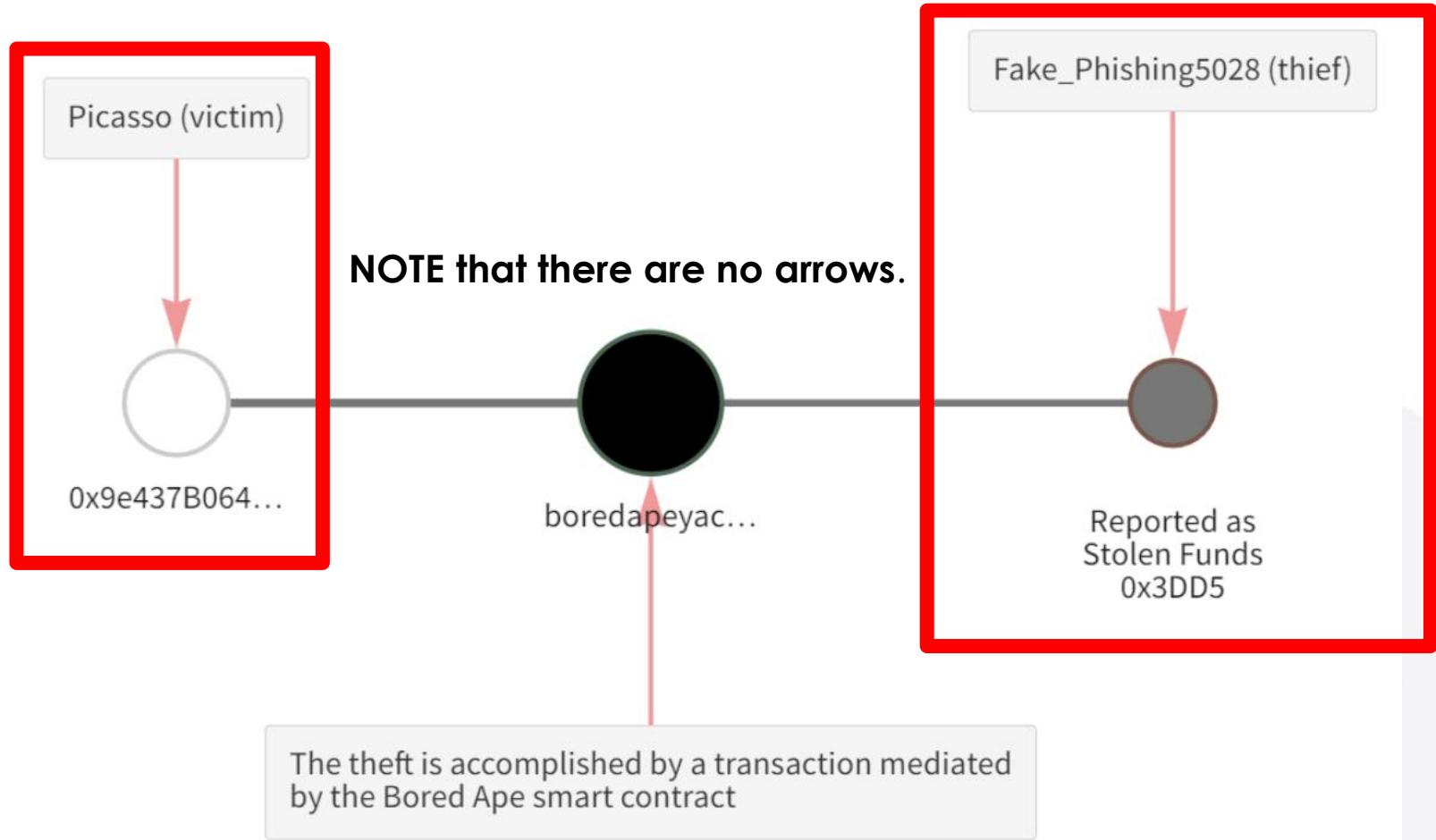
Contract [0x0dc4caueda/b4/abab/c20b1c2e118a18a9... 130](#) (Bored Ape Yacht Club)

0x3dd59de66e2ad31a7d663df977ddd6e5f2a5f6b6

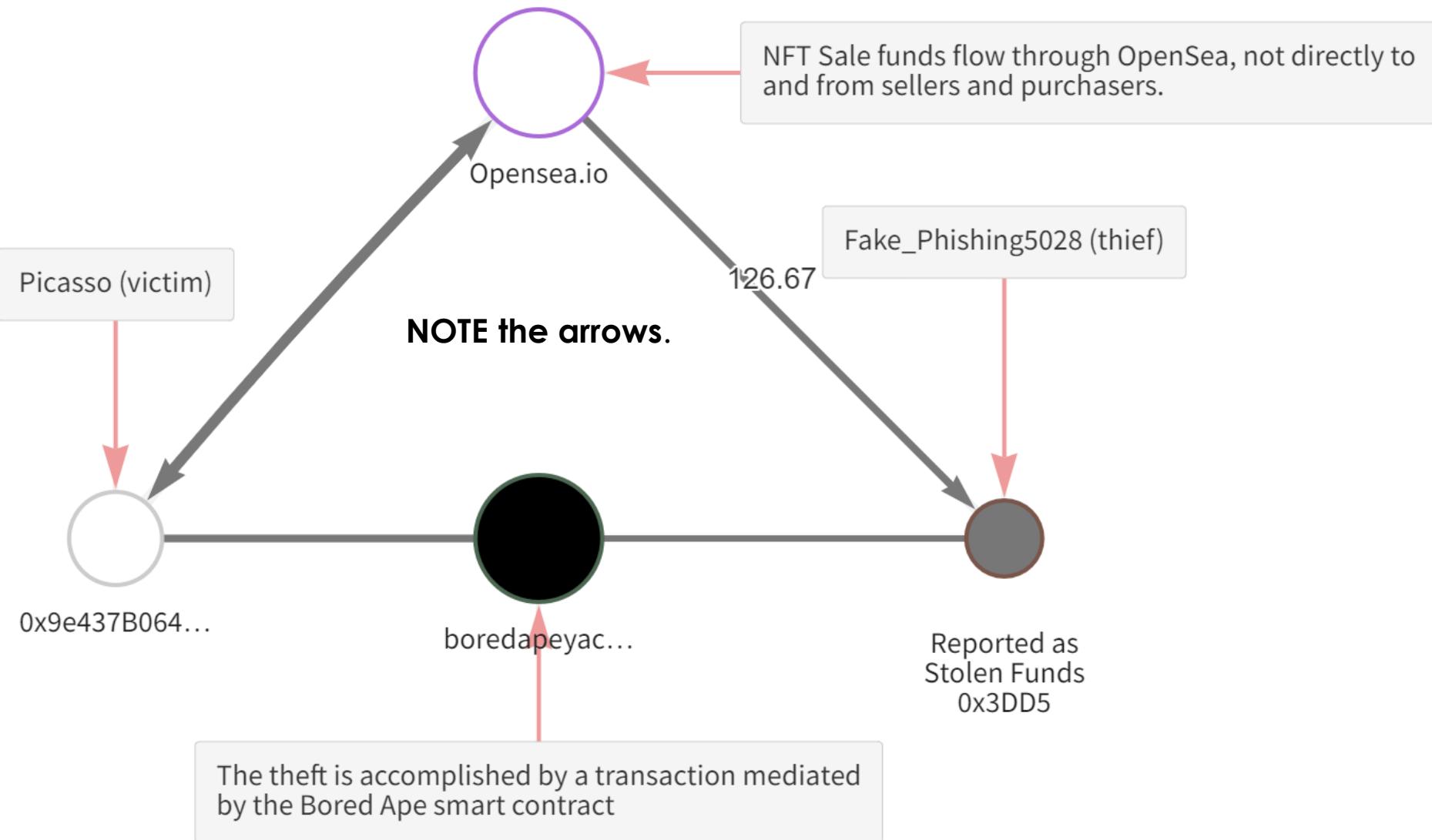
From [0x9e437b064cf... 130](#) To [Fake\\_Phishing5...](#)  
For ERC-721 Token ID [9410] BoredApeYachtClub (BAYC)



# Token Transfer is mediated by the token contract

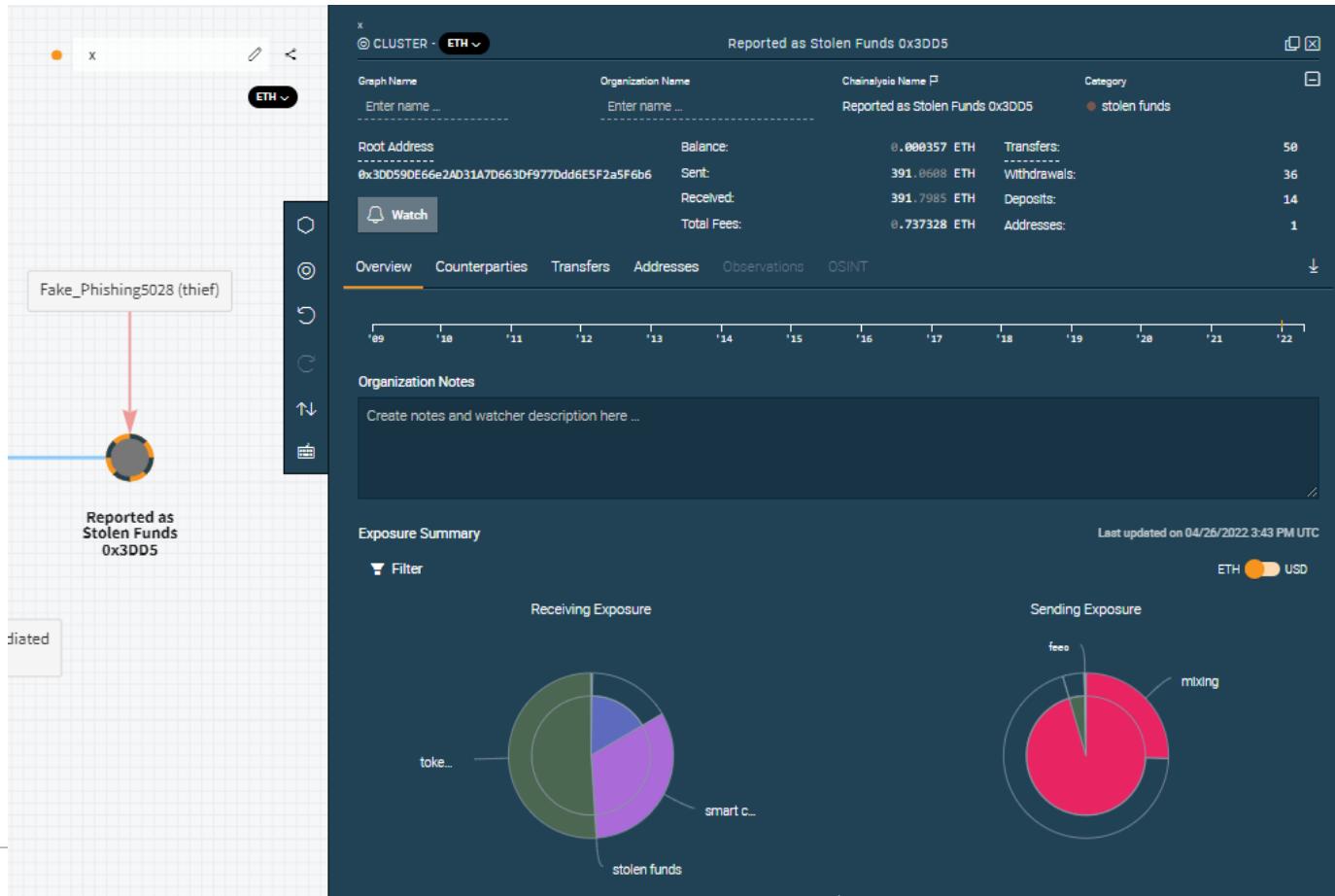


# Money (ETH) goes through OpenSea



# Graph and analyze the thief's address activities

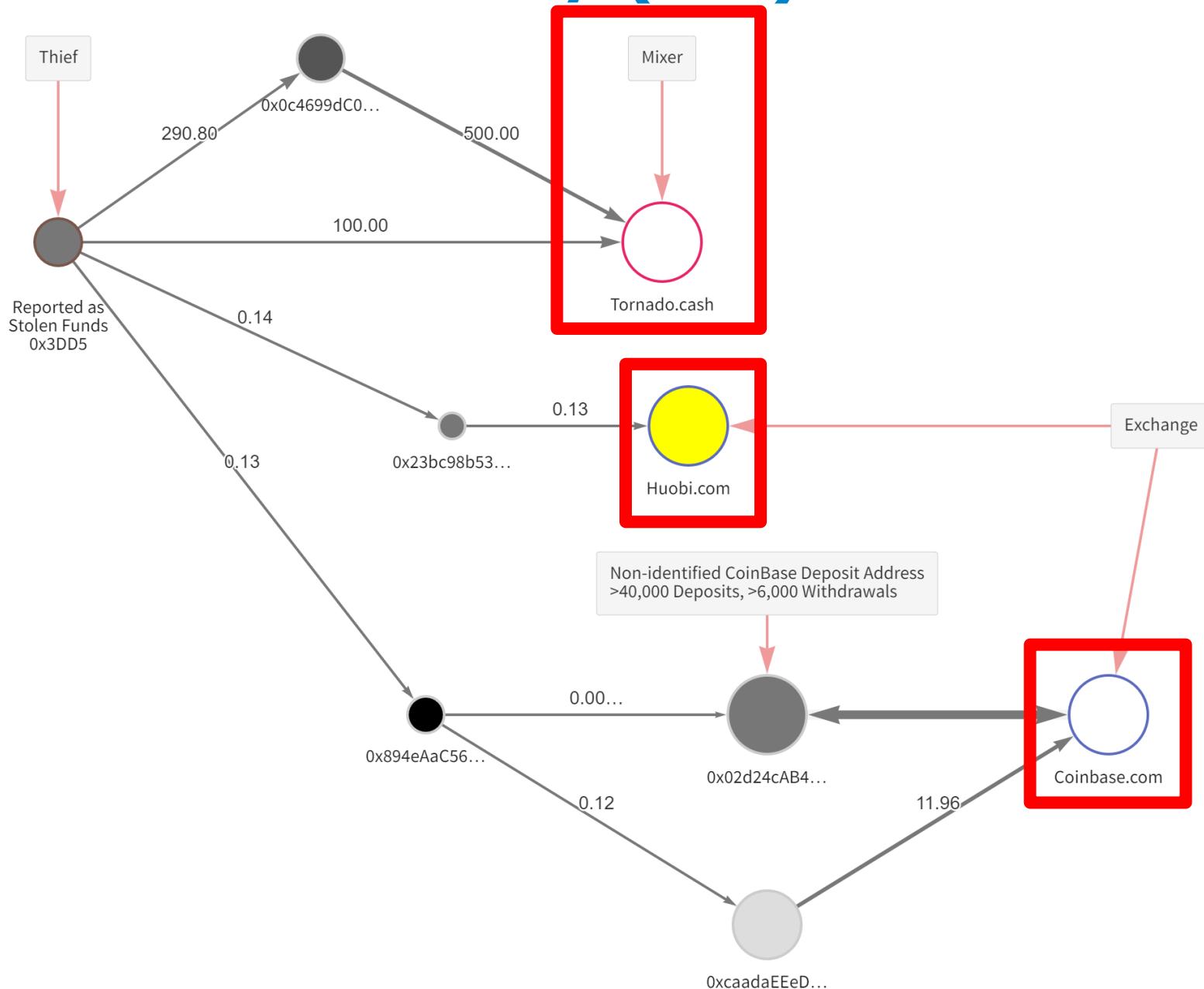
**0x3DD59DE66e2AD31A7D663Df977Ddd6E5F2a5F6b6**



# Thief's Transactions

Counterparty	Transfers	Sent	Received	12/21	12/21
Opensea.io	21	0.00	126.6725		
Wrapped Ether Contract	11	0.00	199.7874		
boredapeyachtclub.com	8	0.00	0.00		
Mutant Ape Yacht Club	1	0.00	0.00		
Sandbox.game	1	0.00	0.00		
0x29aDaa4bBef7F689F5e4Ab2c645F12...	1	0.00	65.00		
0x0c4699dC0d169a8f015351Db285f48...	1	290.7984	0.00		
0x23bc98b530BDF1b2471350159e2C3b...	1	0.136586	0.00		
0x894eAaC56862C9aD4F182A6Eba6051...	1	0.125885	0.00		
collectvox.com v2 (Mirandus)	1	0.00	0.00		
Tornado.cash	1	100.00	0.00		
CloneX Token	1	0.00	0.00		
Reported NFT theft 0xA81db3	1	0.00	0.338662		

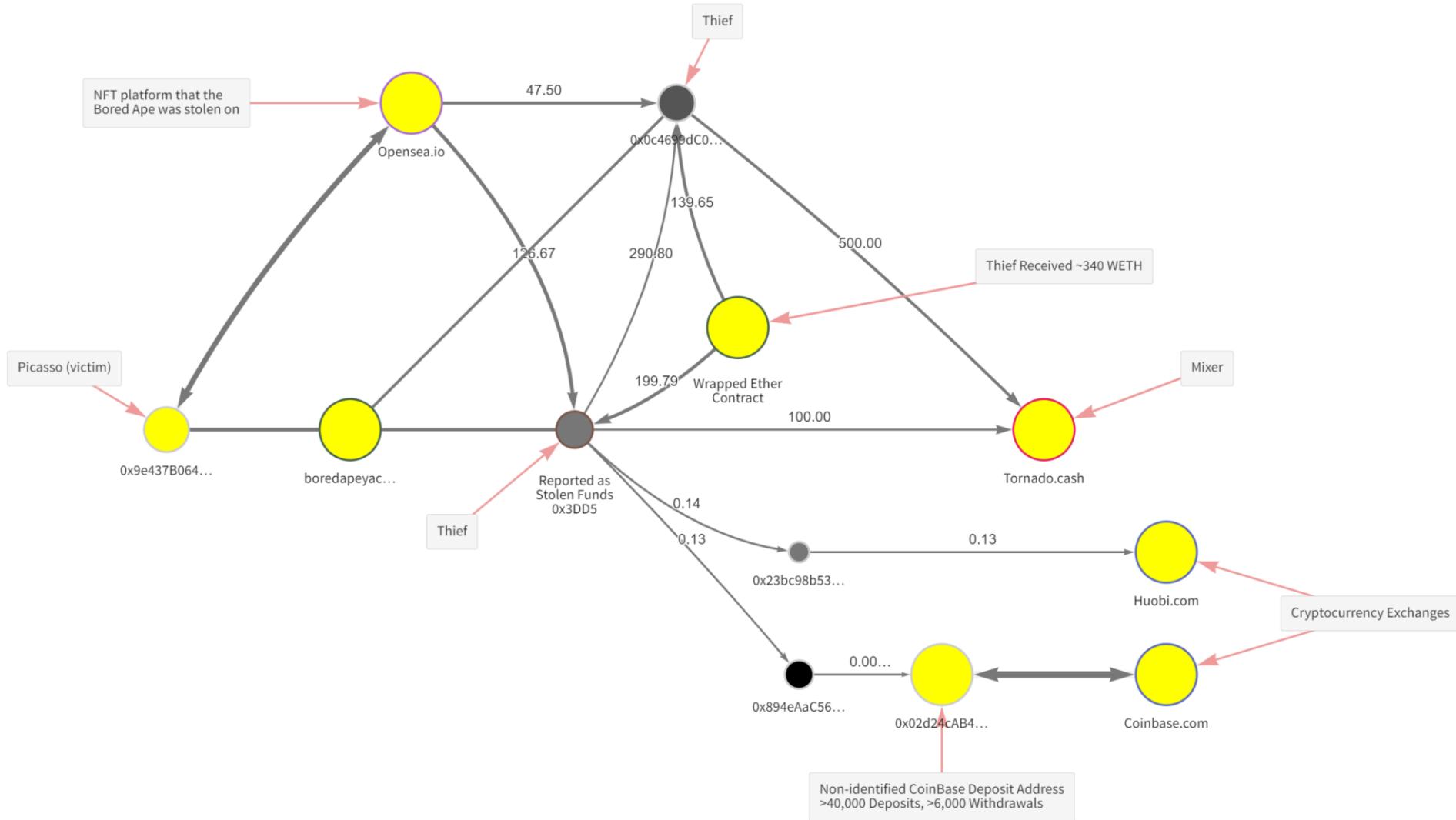
# Follow the Money (ETH)



# Follow the money

- **Exchanges?**
  - KYC information from Huobi?
  - KYC information from Coinbase?
- **Attempt to trace through Tornado Cash?**
  - **TRM Labs offers some ability to trace through Tornado Cash.**
  - **Other suspect addresses may have crypto flowing into them from Tornado Cash** (these might match up with the thief's outflows to Tornado Cash)
    - If these addresses connect to Exchanges, you can use production orders for KYC

# Token interactions with smart contracts + ETH flow = Big Picture



# Investigation Tips

- **Follow the money.** Who benefits?
- **Crypto flows are becoming more sophisticated:** interaction with smart contracts, different tokens, mixing, cross-chain swaps.
- Check for any the **other tokens that were held by the same address.**
- **TornadoCash trace-through** is getting better; some tools may be helpful, new techniques are being developed.

# Investigation Tips

- **Some wallets gather IP addresses and other transaction info** (e.g. **MetaMask**) and are **LE** friendly.
- **NFT platforms gather a lot of information.**
- **VPN connections sometimes drop** and real IPs get revealed.
- **OSINT is a huge source of data:** Twitter (e.g. Rugpullfinder), Facebook, Reddit, Discord, etc.

**Everyone makes mistakes somewhere...**

# POSTSCRIPT

# Bored Ape #9410 was returned to Picasso with the assistance of community members.

Transaction	From	To
Transfer (Theft)	Picasso	3DD59D
Transfer	3DD59D	0x0888_Capital
Sale (82 WETH)	3DD59D	0x0888_Capital
Transfer	0x0888_Capital	C310E7
Transfer	C310E7	0x0888_Capital
Transfer	0x0888_Capital	C310E7
Transfer	C310E7	0x0888_Capital
Transfer	0x0888_Capital	C310E7
Transfer	C310E7	0x0888_Capital
Transfer	0x0888_Capital	C310E7
Transfer	C310E7	0x0888_Capital
Transfer	0x0888_Capital	C310E7
Transfer	C310E7	0x0888_Capital
Transfer	0x0888_Capital	C310E7
Transfer	C310E7	F27628
Transfer	F27628	C310E7
Transfer (Return)	C310E7	<u>Picasso_is_back</u>
Transfer	<u>Picasso_is_back</u>	Picasso
Transfer	Picasso	<u>capetaintrippy</u>
Sale (169.69 ETH)	Picasso	<u>capetaintrippy</u>
Transfer	<u>capetaintrippy</u>	<u>CapetainTrippyVault</u>

# And then more apes were stolen...

Crime

Hackers Broke Into Bored Ape Yacht Club's Official Instagram and Made Off With Nearly \$3 Million Worth of Stolen NFTs

It's not the first time hackers have targeted apes.

Eileen Kinsella, April 26, 2022

