



Cryptocurrency & NFT OSINT

Introduction to Web3/Ethereum
Profiling & Deanonimization

Summary

- Introduction to Blockchain & NFT
- Web3 OSINT
 - On-chain & Off-chain
 - Example
- Use-cases
 - Public Personality Profiling & Analysis
 - Bernard Arnault & family
 - Rug-Pull Victims Identification
 - Frosties
 - Animoon
 - Tornado Cash
 - User statistics & Deanonymization
- Conclusion & Future



Who are we?



- **Patrick Ventuzelo** ([@Pat_Ventuzelo](#))
 - CEO & Founder of Fuzzinglabs
 - Senior Security Researcher
- Specialized in
 - Fuzzing, vulnerability research, and reversing.
 - **Rust**, **Go**, **Blockchain**, **Wasm**, & **Browser** security.
 - Speaker & trainer at various security conferences:
 - BlackHat USA, OffensiveCon, REcon, etc.



- **Tanguy Laucournet**
 - Security Engineer
 - Blockchain/OSINT expert
- Specialized in
 - **Blockchain**, cryptocurrencies, NFTs, etc.
 - Scripting & **Python** development for data analysis
 - **Investigations**, profiling, and de-anonymization related to blockchains

Introduction to Blockchain & NFT

Peer-to-peer (P2P) network

- “Blockchains are **politically decentralized** (no one controls them) and **architecturally decentralized** (no infrastructural central point of failure) but they are **logically centralized** (there is one commonly agreed state and the system behaves like a single computer)” - [Vitalik Buterin](#)

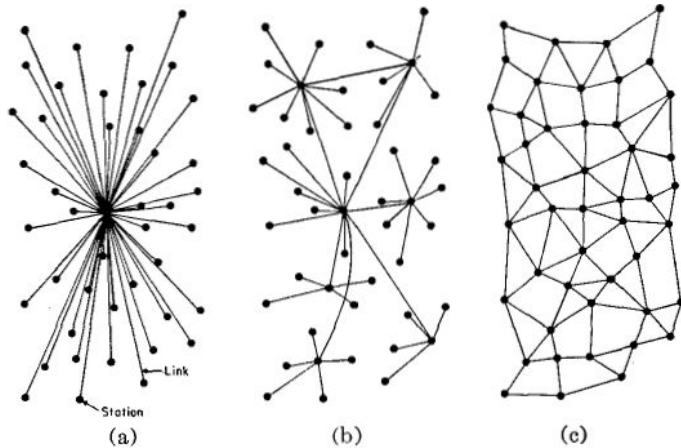
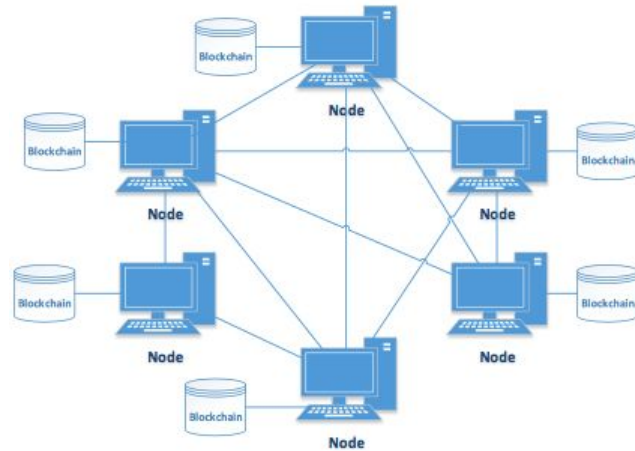


Fig. 1—(a) Centralized. (b) Decentralized. (c) Distributed networks.



Block + chain

- **Addresses**

- Public key
- **Unique identifiers**
 - Ex: 0x21a06d452a1f49f55635ecac61348df606ed9bae

- **Transaction**

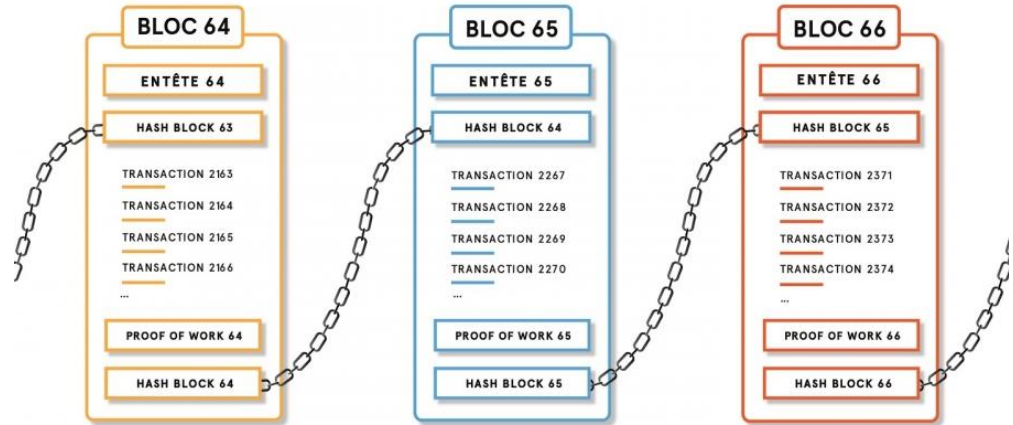
- Interaction between participants
- Ex: Address A send money to Address B

- **Block**

- Set of transactions between accounts

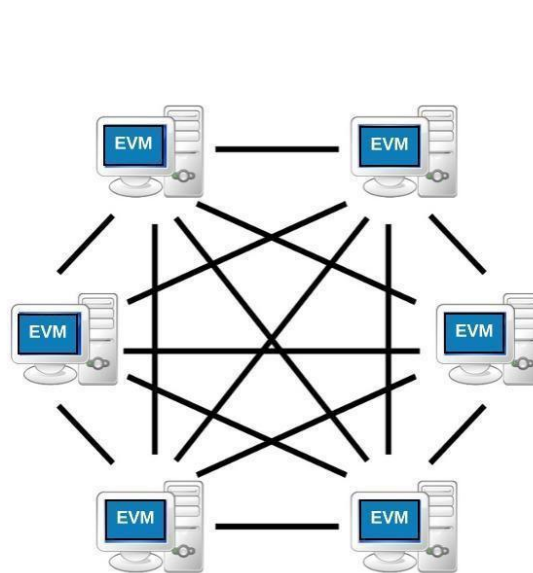
- **Blockchain**

- Series of blocks
 - each linked to the previous block
- **Immutable** public transaction ledger
- Stored forever in the blockchain



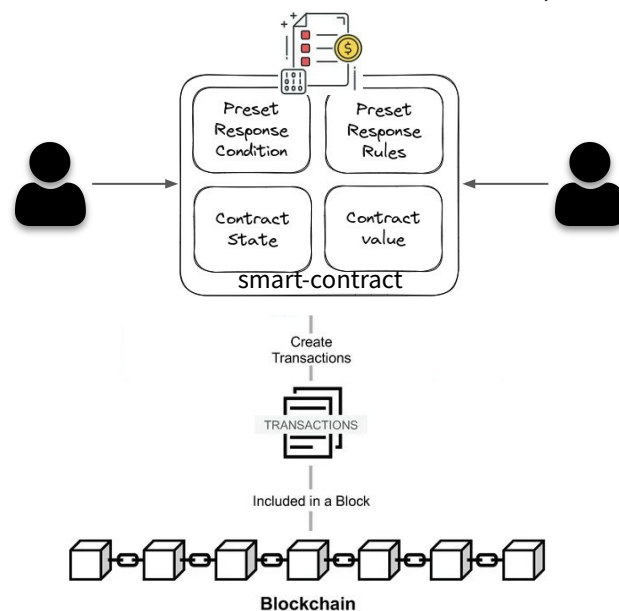
What is Ethereum?

- Ethereum is a **decentralized platform** that **runs smart contracts**: applications that run exactly as programmed without any possibility of downtime, censorship, fraud, or third-party interference.
- Created by Vitalik Buterin, Gavin Wood, etc.
- [Open source](#)
- Decentralized **cryptocurrency**
- Decentralized network (P2P)
 - launched on 30 July 2015
 - **Public data 24 hours a day, 7 days a week.**
- Consensus
 - Proof of work (PoW)
 - Since September 2022: **Proof of Stake (PoS)**
- **Ethereum Virtual Machine (EVM)**
 - Sandboxed virtual stack machine



What is a Smart Contract?

- “A smart contract is a **computer program** or a **transaction protocol** which is intended to **automatically execute, control** or document legally relevant events and actions according to the terms of a contract or an agreement. The **objectives of smart contracts are the reduction of need in trusted intermediates, arbitrations and enforcement costs, fraud losses**” - [Wikipedia](#)
- Ethereum Smart Contracts
 - Written in Solidity.
 - **DApps** (Decentralized Application)
 - Stored on the blockchain
 - Executed by the EVM

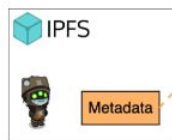


What is a NFT (Non-fungible token)?

- An **NFT (Non-fungible token)** is a digital asset that can be used to represent all kinds of things on a blockchain.
 - ERC-721 standard

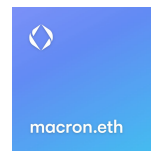
Token ID	Owner's Address
12	0x3a058...aD56A

Token ID	Token Meta Data URI
12	ipfs://bafybeic3ui4dj5d...tefgq/metadata.json



```
{  
  "name": "my cool avatar #12"  
  "description": "very cool ninja avatar"  
  "image": "ipfs://bafybeihii26gwp....d3fq/ninja-avator.png"  
}
```

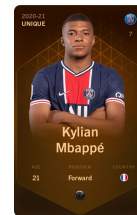
- Key features:
 - Immutability
 - Transparency
 - Can be owned and transferred
 - Indivisible
 - **Uniqueness**



ENS



Profile Picture



Sport



POAP



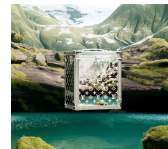
Ticketing



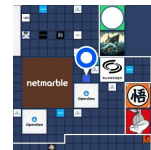
Art



Gaming



Luxury



Metaverse

Web3 OSINT Usage & Analysis

Web3/Cryptocurrencies OSINT in the wild

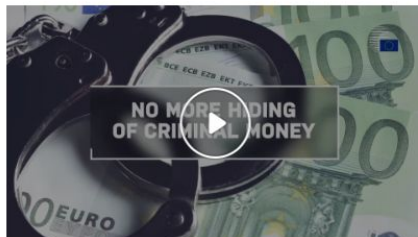
PRESS RELEASES

U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash

Council of the EU Press release 16 May 2023 10:30

Anti-money laundering: Council adopts rules which will make crypto-asset transfers traceable

The EU is making it more difficult for criminals to circumvent anti-money laundering rules via crypto currencies. Today the Council adopted updated rules on information accompanying the transfers of funds by **extending the scope of the rules to transfers of crypto assets**. This ensures financial transparency on exchanges in crypto-assets and provides the EU with a solid framework that complies with the most demanding international standards on the exchange of crypto-assets, ensuring that these are not used for criminal purposes.



The EU is making it more difficult for criminals to misuse crypto-assets for money laundering purposes

Five Charged in France With \$2.5M Fraud Targeting Bored Ape NFT Owners

Noted online crypto sleuth "ZachXBT" played a key role in helping French authorities uncover the fraudulent Bored Ape NFT scheme.

By Will McCurdy

Oct 13, 2022

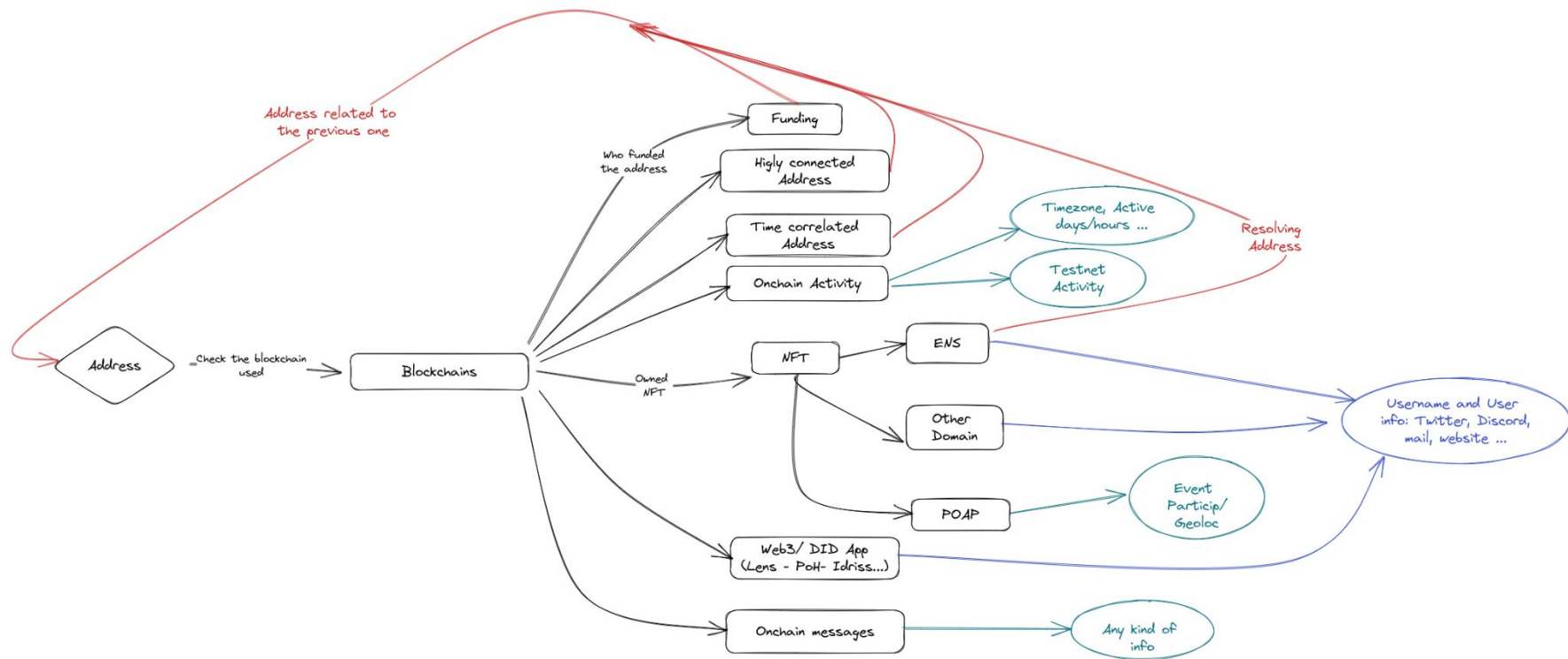
3 min read



Bored Ape Yacht Club NFTs have become one of the most popular collections in crypto. Image: Shutterstock.

[link](#)
[link2](#)
[link3](#)

Wallet Address to Identity - **On-Chain** analysis

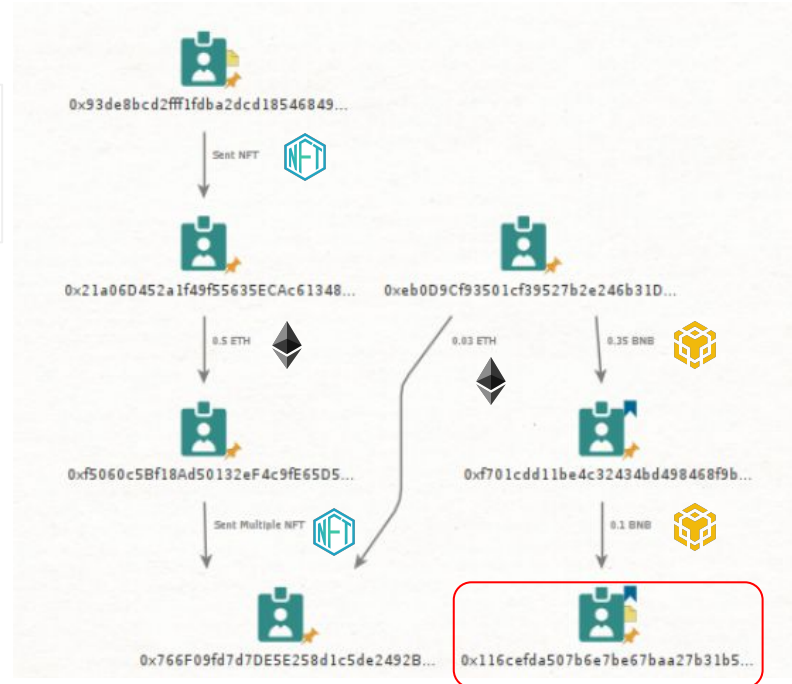


Example: Analysis of the 0x116cef...

- Address: [0x116cefda507b6e7be67baa27b31b5f5ceabea154](#)
 - Mentioned in [Aleno's blogpost](#) about the Euler hack

For each address, we conducted a behavioral and transactional analysis to analyze the habits of the addresses and we found that [0x116ce](#) has really **suspicious behavior**.

- Multi-chain interactions
 - Exchange ETH over Ethereum
 - Exchange BNB over BNB Smart Chain
 - Exchange NFT over Ethereum
- **Is it enough to assume there are linked together?**



Example: 0x116 relationships

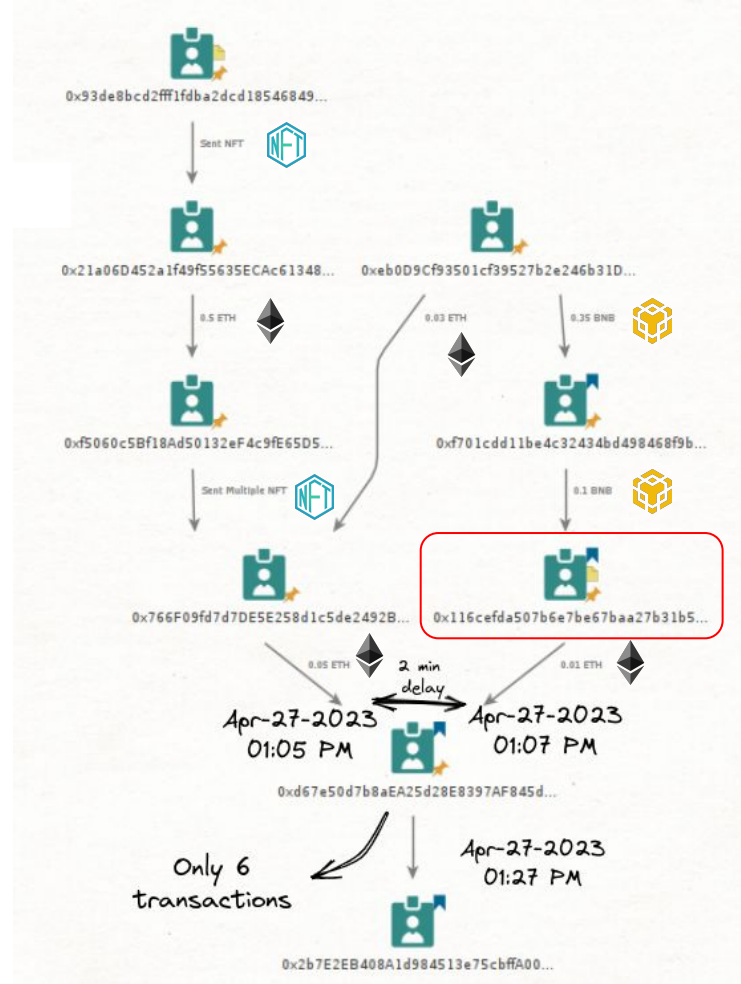
- **Is it enough to assume there are linked together?**

- Depends of how strong is the wallet's relationship
- In this case, we have in/out transactions with 0x766F
 - I.e. [0xd67e50d7b8aea25d28e8397af845da808fb47ba1](#)

Latest 6 from a total of 6 transactions

Export Current Page Data Advanced Filter

Method	Block	Age	From	To	Value
Any Swap Out...	17137807	60 days 1 hr ago	0xd67e50...8fb47BA1	Multichain: Router V6	0.101 ETH
Transfer	17137707	60 days 1 hr ago	0x116cEF...eAbEa154	0xd67e50...8fb47BA1	0.01112823 ETH
Transfer	17137696	60 days 1 hr ago	0x766F09...30344d6B	0xd67e50...8fb47BA1	0.052856 ETH
Deposit	17043001	73 days 10 hrs ago	0xd67e50...8fb47BA1	Tornado.Cash: Router	1 ETH
Deposit	16981867	82 days 4 hrs ago	0xd67e50...8fb47BA1	Tornado.Cash: Router	1 ETH
Transfer	16981854	82 days 4 hrs ago	0x526b78...20081D24	0xd67e50...8fb47BA1	0.00980455 ETH



Example: Wallet's ENS relationships

- Addresses:





- [0x21a06d452a1f49f55635ecac61348df606ed9bae](#)
- [0xf5060c5Bf18Ad50132eF4c9fE65D52eBc55ee025](#)
- [0x766f09fd7d7de5e258d1c5de2492b2d530344d6b](#)

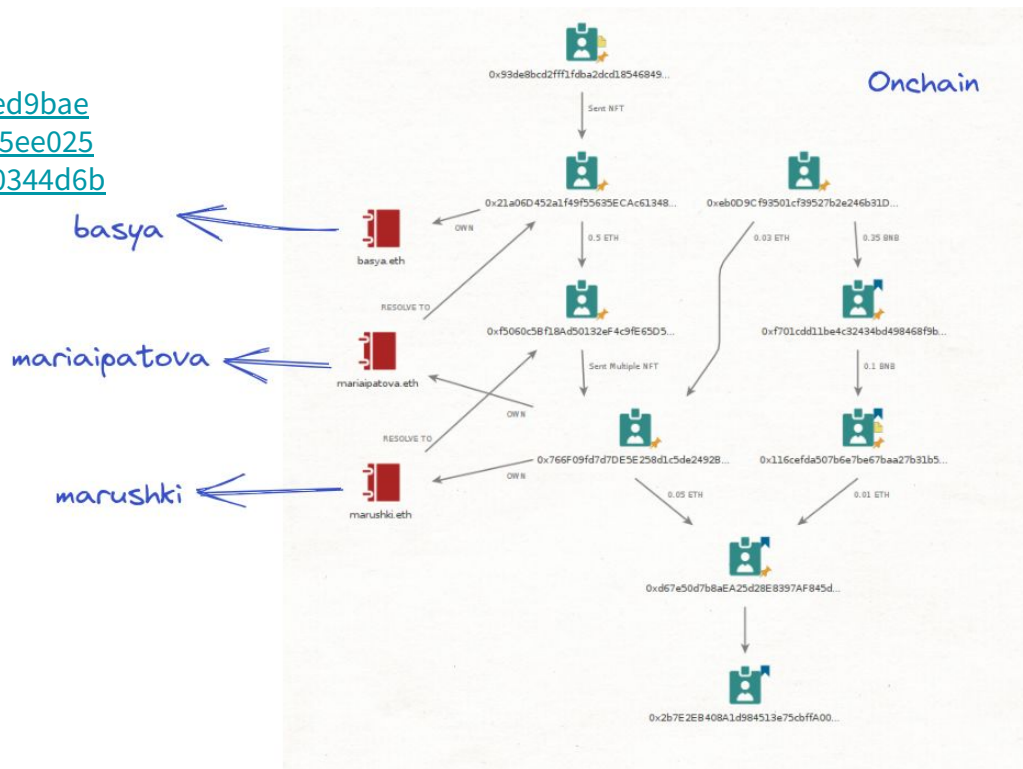
- Domain Name Lookup

- **ENS**
- Unstoppable Domains

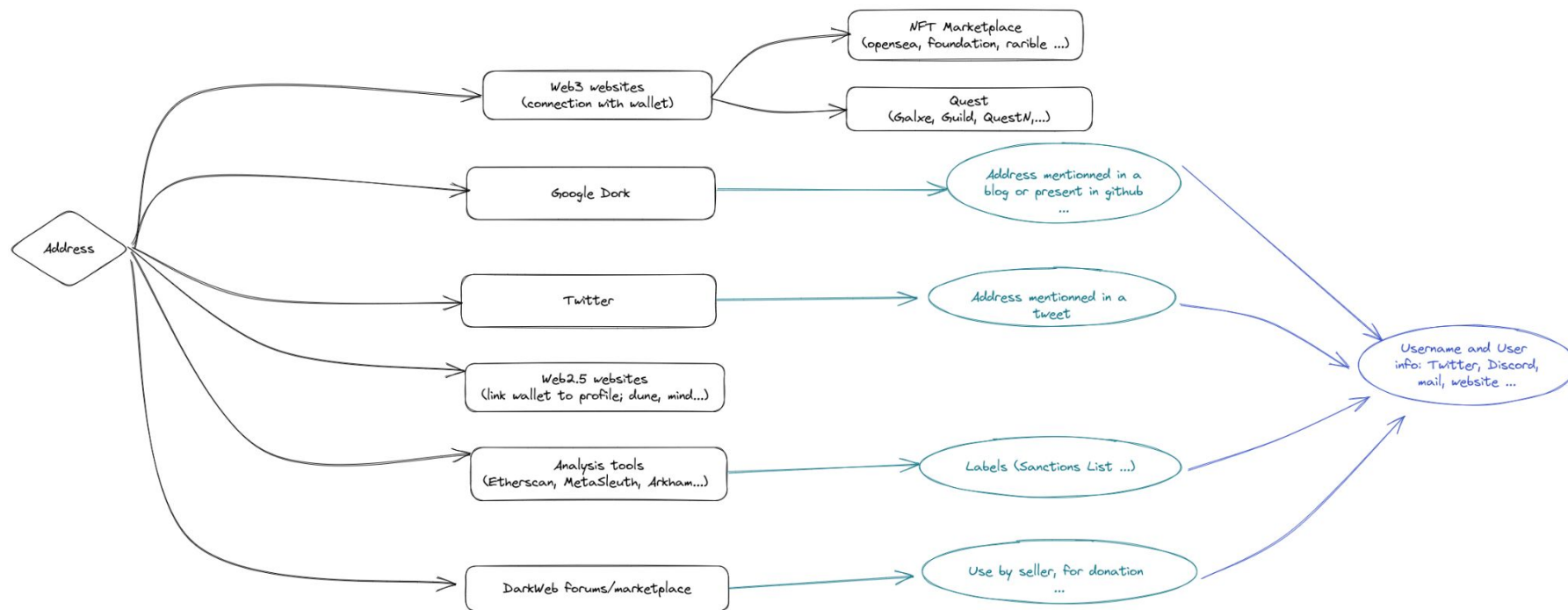
Result for: **mariaipatova.eth**

Overview of ENS

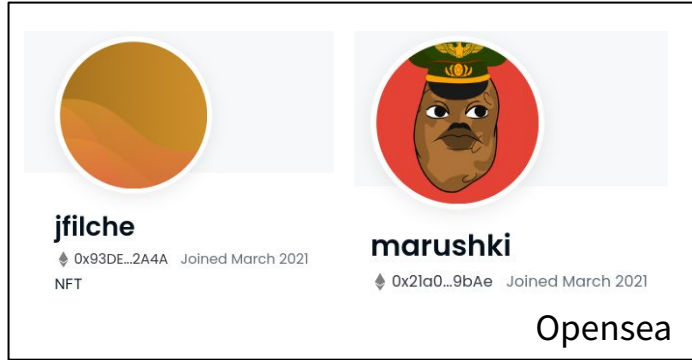
Resolved Address:	 0x21a06D452a1f49f55635ECAc61348dF606Ed9bAe
Expiration Date:	 2027.01.07 at 11:26
Registrant:	0x766F09fd7d7DE5E258d1c5de2492B2d530344d6B 
Controller:	0xf5060c5Bf18Ad50132eF4c9fE65D52eBc55ee025 



Wallet Address to Identity - **Off-chain** Analysis



Example: Identities behind those wallets



jfilche
0x93DE...2A4A Joined March 2021
NFT

marushki
0x21a0...9bAe Joined March 2021

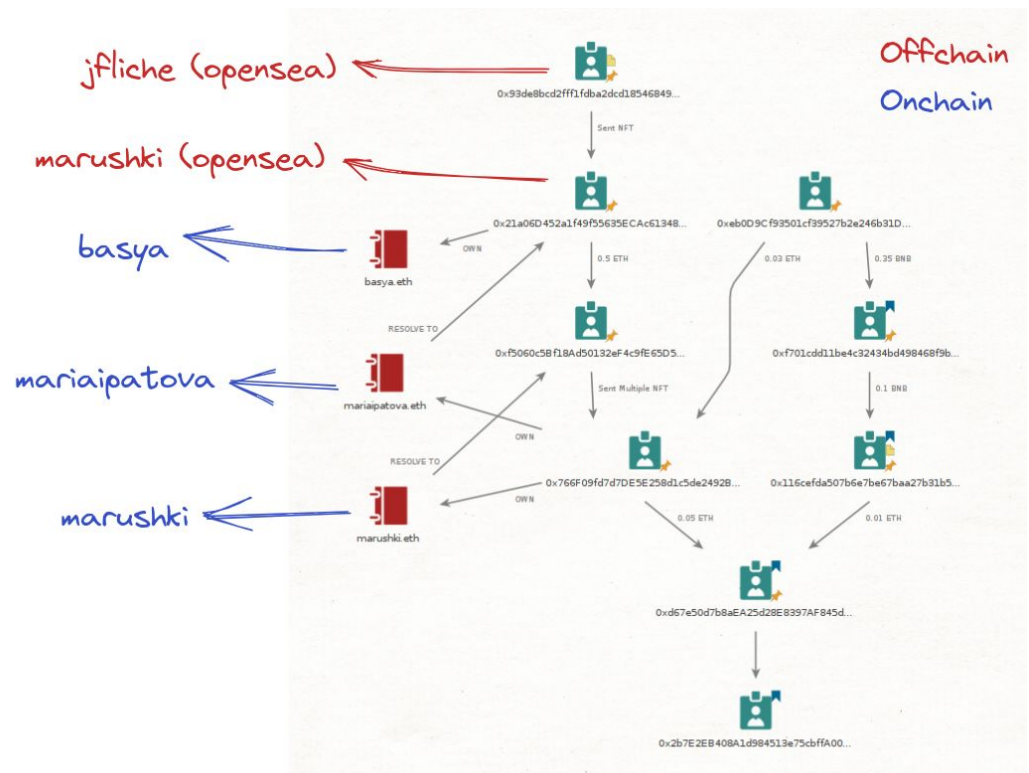
Opensea



Julian
@Jfilche

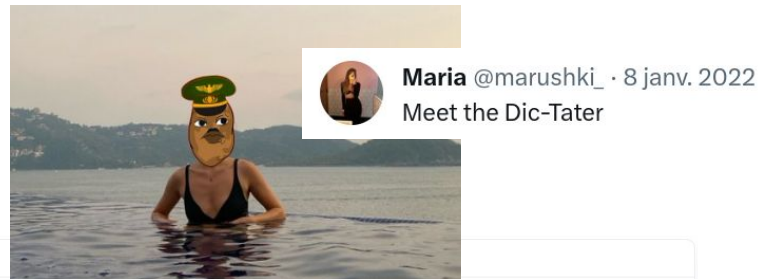
Maria
@marushki_

Twitter



Example: How to confirm it's the same people/friends?

- Maria made a tweet about a [TOONZ #5081](#)
 - In April 2022, 0x21a6 was the owner of this NFT



Item Activity

A total of 9 records found

Txn Hash	Age	Action	Price	From	To
0xd0d6f3b0c766cfa2...	39 days 5 hrs ago	Sale	0.189 ETH (\$347.71)	0xb813f3...E9f2C6C5	0xwn.eth
0x5ae1e153592c4539...	39 days 19 hrs ago	Sale	0.20801 WETH (\$382.68)	0xDadD6e...E9f2C6C5	0xb813f3...E9f2C6C5
0xe672b4b196c45ec2...	39 days 19 hrs ago	Sale	0.2 Blur Pool	david-taylor.eth	0xDadD6e...E9f2C6C5
0x09c9bb8e84981d41...	113 days 8 hrs ago	Sale	0.6 ETH (\$1,103.83)	0x3Dd932...e2a937Ba	david-taylor.eth
0x1269f67e284e29269...	122 days 7 hrs ago	Sale	0.52 Blur Pool	suthie.eth	0x3Dd932...e2a937Ba
0x8c2b618ac3d2120d...	122 days 10 hrs ago	Sale	0.57 ETH (\$1,048.63)	0x766F09...30344d6B	suthie.eth
0xfefadafe5bef88a84c...	122 days 21 hrs ago	Transfer		0xf5060c...c55ee025	0x766F09...30344d6B
0xa3f7ab66a3e51c665...	170 days 14 hrs ago	Transfer		0x21a06D...06Ed9bAe	0xf5060c...c55ee025
0x684b601f512447a07...	472 days 3 hrs ago	Mint		Null: 0x000...000	0x21a06D...06Ed9bAe

Use-cases

Public Personality Profiling & Analysis

Bernard Arnault owns NFTs?

- Ian Rogers (Former chief digital officer at LVMH)
 - Say during Aarthi and Sriram's Good Time Show podcast.
- “I don't think he'd mind if I said this—**he has shown me**, of his own volition, **his OpenSea page**,” said Rogers, referencing a digital NFT marketplace. “Which means he had to pull out his phone, find it, and then take me through it. So, yes.”
- **Let's try to find Bernard's NFT Wallet!**
- Source: Observer - [link](#)

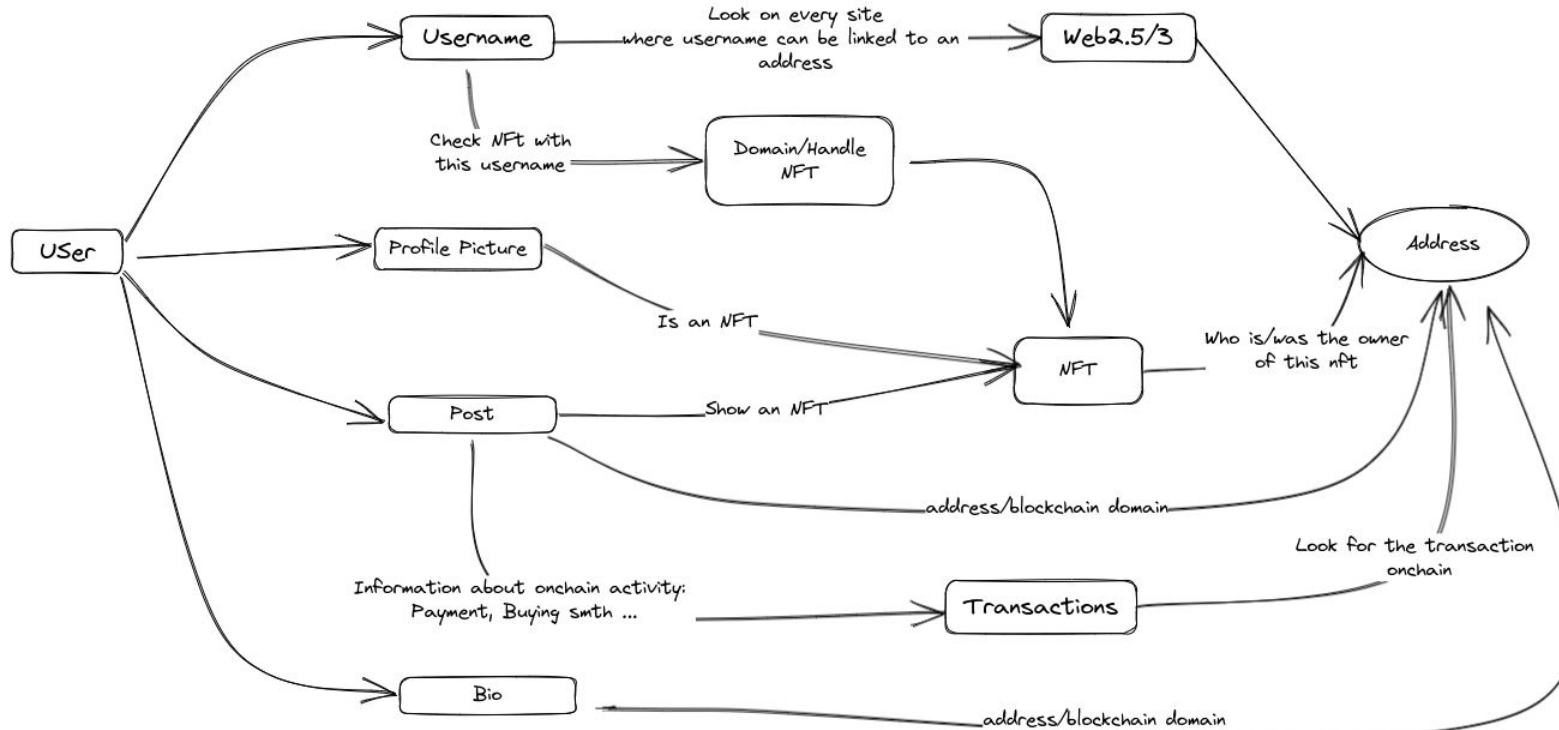
LVMH's Bernard Arnault Has a Secret NFT Collection

The billionaire is a prominent art collector and opened a private museum but has expressed doubts about digital artwork as an investment.

By [Alexandra Tremayne-Pengelly](#) · 05/03/23 2:48pm



User to Wallet Address - Process overview



Arnault's family & LVMH ❤️ NFTs

- Frederic Arnault - [Twitter](#)
 - CEO of watch brand Tag Heuer



- Alexandre Arnault - [Twitter](#)
 - CEO of jewelry brand Tiffany & Co.



How to find the wallet behind an NFT?

- NFT Reverse Image Search
 - [Fingible](#)
 - [NFT Finder](#)
 - [Bing.ly](#)
 - Not working well with a screen capture
- Google image search
 - <https://images.google.com/>
 - look for NFT marketplace results
- OpenSea/Marketplace
 - Trait filtering - [link](#)
- AI Image Similarity is your friend 😊

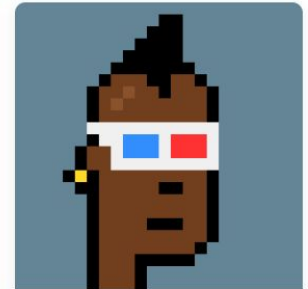


CryptoPunk #3167

Last sale: 160 ETH



CryptoPunk #3180



CryptoPunk #3209

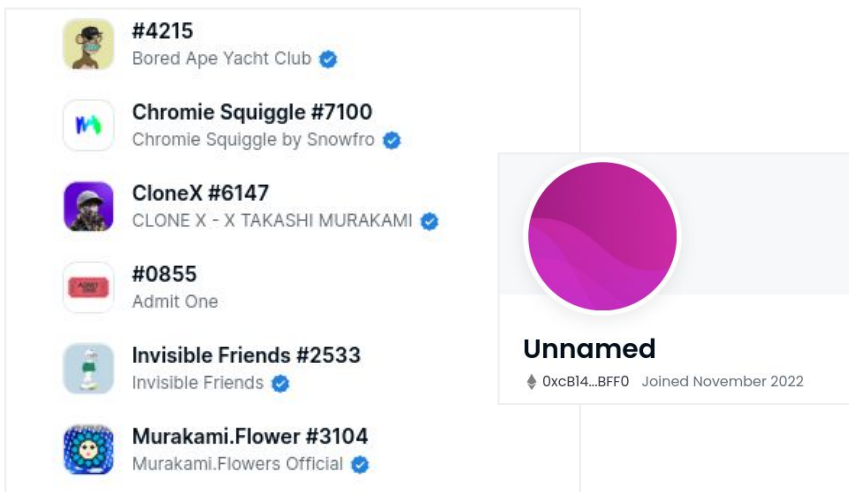
Last sale: 104.99 ETH

<input checked="" type="checkbox"/>	3D Glasses	286
<input checked="" type="checkbox"/>	Male	6,039

OpenSea Profiles

Frederic

- Address: [0xcB142075Ae31E89D939B74494415B3d7d9b0BFF0](https://etherscan.io/address/0xcB142075Ae31E89D939B74494415B3d7d9b0BFF0)
- OpenSea Profile - [link](#)

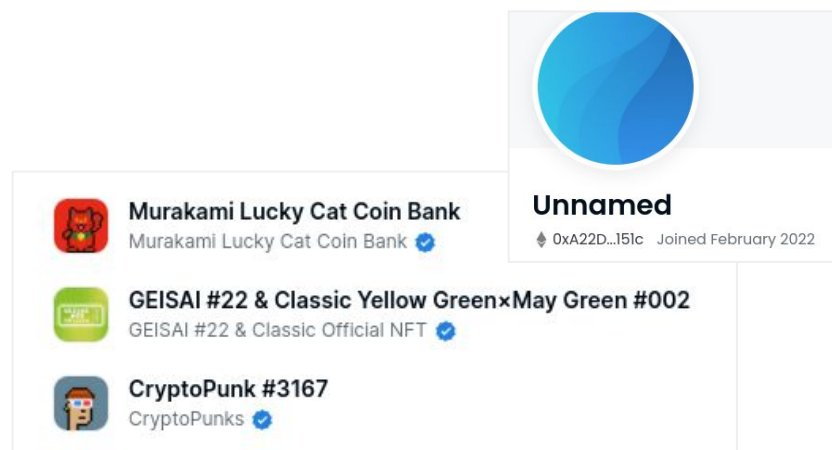


A screenshot of an OpenSea profile for a user named 'Unnamed'. The profile features a purple circular avatar and a bio that reads '0xcB14...BFF0' and 'Joined November 2022'. To the left of the profile is a list of six collections:

- #4215 Bored Ape Yacht Club
- Chromie Squiggle #7100 Chromie Squiggle by Snowfro
- CloneX #6147 CLONE X - X TAKASHI MURAKAMI
- #0855 Admit One
- Invisible Friends #2533 Invisible Friends
- Murakami.Flower #3104 Murakami.Flowers Official

Alexandre

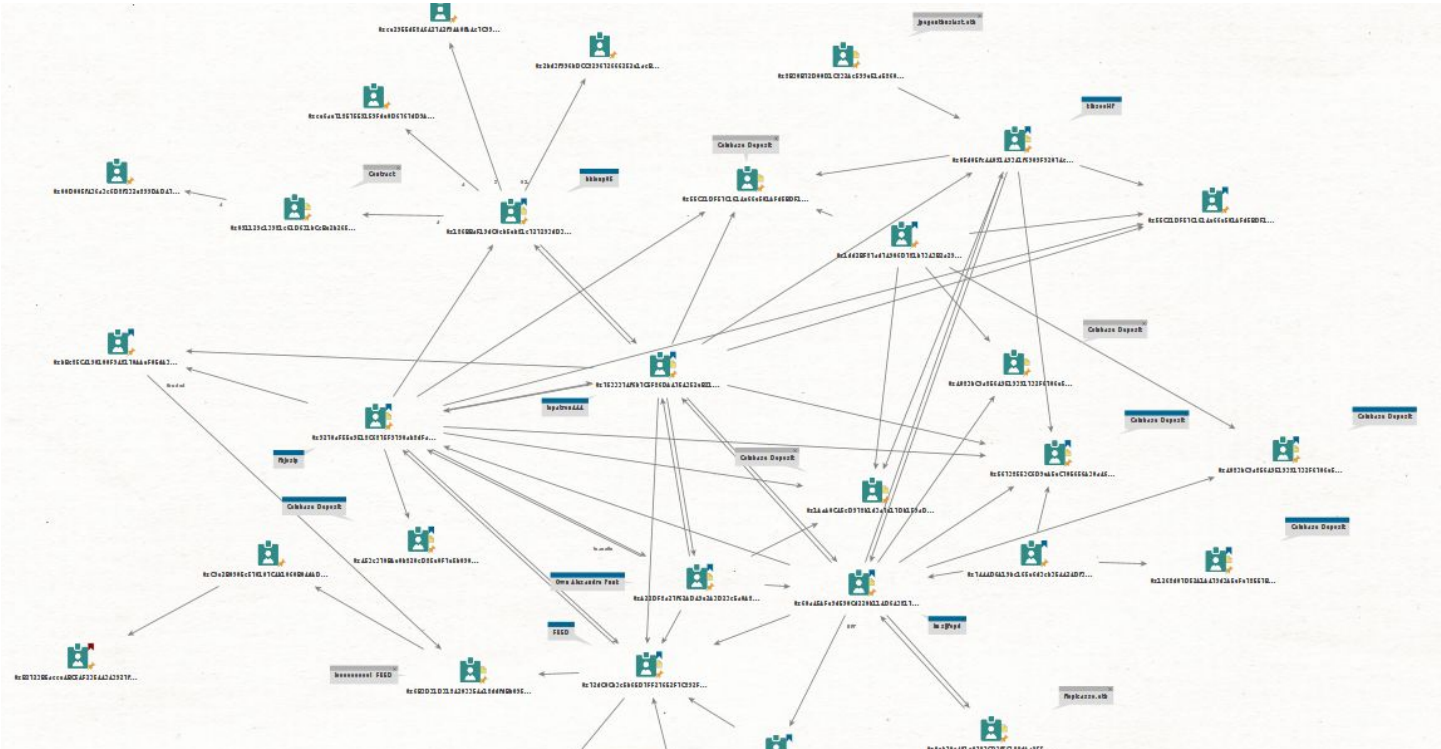
- Address: [0xa22df8a27f62ad49e2a3d23cea0a86421ec1151c](https://etherscan.io/address/0xa22df8a27f62ad49e2a3d23cea0a86421ec1151c)
- OpenSea Profile - [link](#)



A screenshot of an OpenSea profile for a user named 'Unnamed'. The profile features a blue circular avatar and a bio that reads '0xA22D...151c' and 'Joined February 2022'. To the left of the profile is a list of four collections:

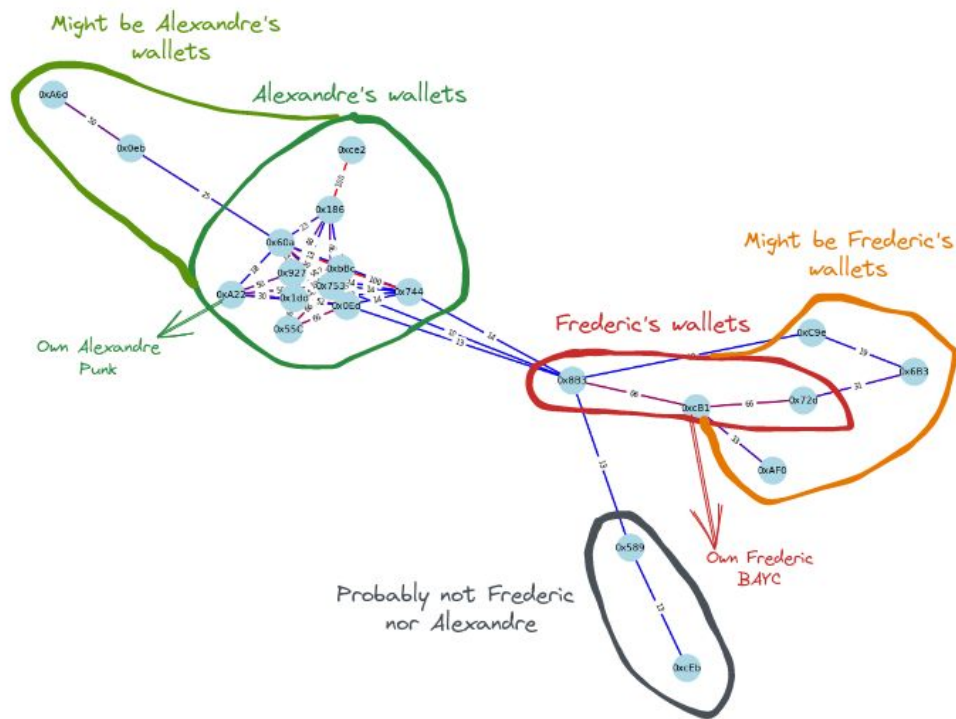
- Murakami Lucky Cat Coin Bank Murakami Lucky Cat Coin Bank
- GEISAI #22 & Classic Yellow GreenxMay Green #002 GEISAI #22 & Classic Official NFT
- CryptoPunk #3167 CryptoPunks

On-chain Analysis



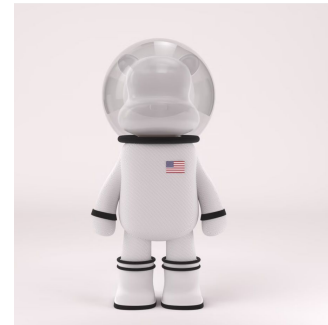
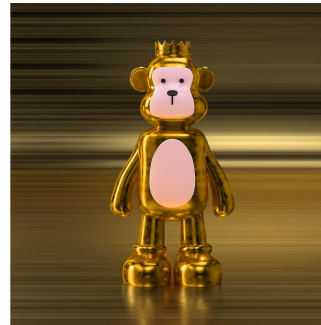
Wallet Clusterization through Time Correlation

- Get all the transactions for each address
- For each transaction from a wallet
 - look for other transactions from other wallets within a **predefined time window**
 - Graph the data with weighted relation based on the **frequency of close interactions between addresses**
- What's the purpose?
 - Differentiate multiple users behind a list of highly connected addresses.
 - Find **all wallets controlled by a single user**.



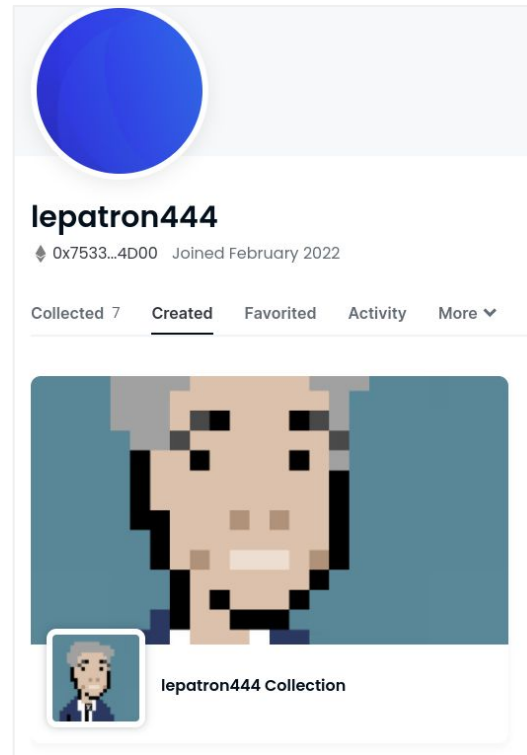
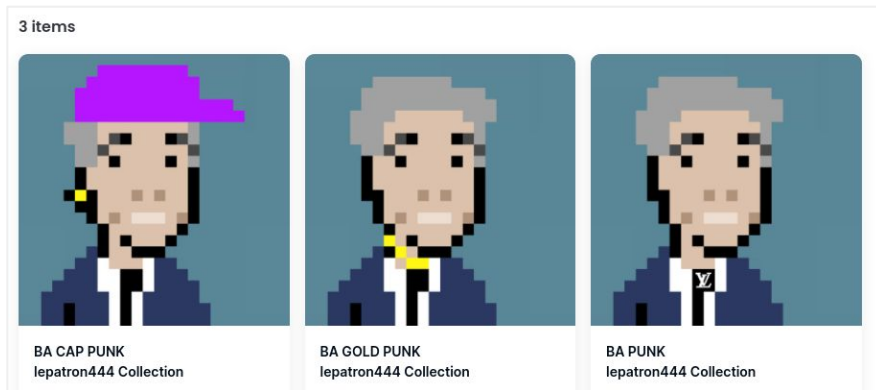
Does Alexandre is doing NFT insider trading?

- Pre-reveal (Blind auction)
 - No one knows the rarity of each NFT
 - Alexandre
 - Bid 32% more to get [#9021](#)
 - Bid 58% more to get [#7777](#)
 - Bid for 7 other NFT
- After Reveal
 - He **bid on 5** of the 10 rarest and **win 3**
 - Sell [#9021](#) for \$14,700
 - 377% gain, **\$11,600 profit**
 - Sell [#7777](#) for \$12,900
 - 330% gain, **\$9000 profit**
 - Use multiple wallets to make the trades
- Could it be random? **Odds are 1/440,000**
 - In comparison, lifetime odds of getting struck by lightning are about 1/15,000
- Source: Forbes Article using Convex Labs analysis - [link](#)



Do we find Bernard Arnault's NFT wallet?

- No, but one of Alexandre's wallets is surprising...
- Address: [0x7533374f6b7CEF86DA4754352eB21Cf2d9664D00](https://etherscan.io/address/0x7533374f6b7CEF86DA4754352eB21Cf2d9664D00)
- Opensea profile: [lepatron444](https://opensea.io/lepatron444)
 - "lepatron" mean "theboss" in French
 - 444 might refer to LVMH's market cap valorization (444 billion)
- This wallet owner created a collection of NFT

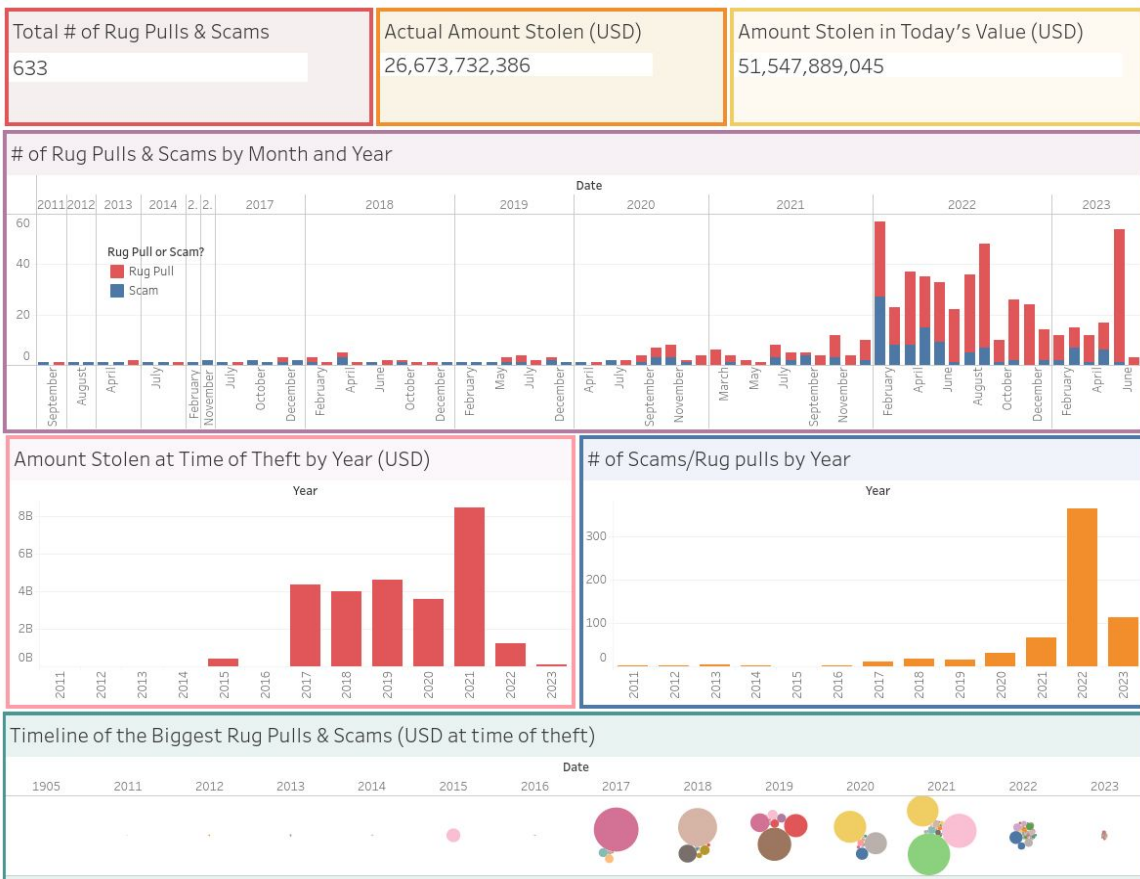


Use-cases

Rug-Pull Victims Identification

What is a Rug-Pull?

- A rug pull is a scam where a cryptocurrency or NFT developer **hypes a project to attract investor** money, only to suddenly **shut down or disappear**, taking investor assets with them.
- The name comes from the idiom “to pull the rug out” from under someone, leaving the victim off-balance and scrambling.
- Source: Comparitech’s Worldwide crypto & NFT rug pulls and scams tracker - [link](#)



Rug-Pull Victims Identification Frosties

What is Frosties?



- One of the first cases of rug-pull charged by the U.S.
 - ~ **\$1.2 Million NFT Fraud Scheme**
- 20 years old founders:
 - Ethan Nguyen & Andre Llacuna
- Got charges for
 - conspiracy to commit **Wire Fraud**
 - conspiracy to commit **Money Laundering**
 - Usage of Tornado Cash
- They were planning to create another one
 - “Embers” for around \$1.5 Million
- Sources: PRESS RELEASE - [link](#), FINAL Complaint - [link](#)

The screenshot shows the official website of the United States Attorney's Office for the Southern District of New York. The header includes the office's name and logo, along with navigation links for 'About SDNY', 'Find Help', and 'Contact Us'. A search bar is visible in the top right. Below the header is a dark navigation bar with dropdown menus for 'About', 'Priorities', 'News', 'Resources', 'Programs', 'Employment', and 'Contact'. The main content area features a breadcrumb trail: 'Justice.gov > U.S. Attorneys > Southern District of New York > Press Releases > Two Defendants Charged In Non-Fungible Token ("NFT") Fraud And Money Laundering Scheme'. The title of the press release is 'Two Defendants Charged In Non-Fungible Token ("NFT") Fraud And Money Laundering Scheme'.

PRESS RELEASE

Two Defendants Charged In Non-Fungible Token (“NFT”) Fraud And Money Laundering Scheme

Thursday, March 24, 2022

Share >

For Immediate Release

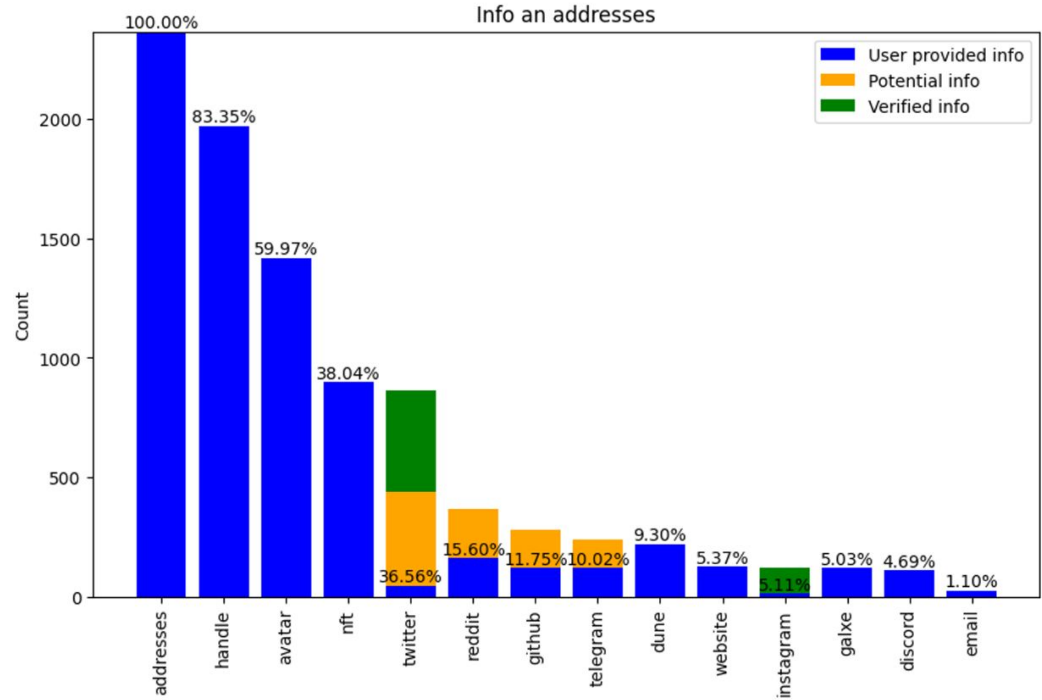
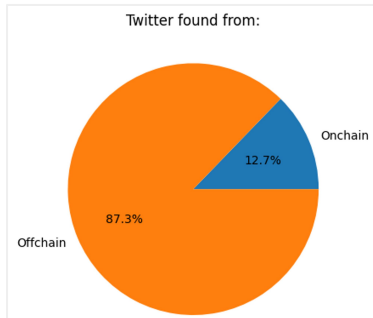
U.S. Attorney's Office, Southern District of New York

Defendants Executed a \$1 Million NFT Fraud Scheme in January 2022, and Were Preparing to Execute a Second Prior to Their Arrests

Damian Williams, the United States Attorney for the Southern District of New York, Thomas Fattorusso, Special Agent in Charge of the New York Field Office of the Internal Revenue Service, Criminal Investigation (“IRS-CI”), Ricky J. Patel, the Acting Special Agent-in-Charge of the New York Field Office of the Department of Homeland Security (“HSI”), and Daniel B. Brubaker, Inspector-in-Charge of the New York Office of the U.S. Postal Inspection Service (“USPIS”), announced that ETHAN NGUYEN, a/k/a “Frostie,” a/k/a “Jakefiftyeight,” a/k/a “Jobo,” a/k/a “Joboethan,” a/k/a “Meltfrost,” and ANDRE LLACUNA, a/k/a “heyandre,” were charged in a criminal complaint with conspiracy to commit wire fraud and conspiracy to commit money laundering, in connection with a million-dollar scheme to defraud purchasers of NFTs advertised as “Frosties.” Rather than providing the benefits advertised to Frosties NFT purchasers, NGUYEN and LLACUNA transferred the cryptocurrency proceeds of the scheme to various cryptocurrency wallets under their control. Prior to their arrests in Los Angeles, California, NGUYEN and LLACUNA were preparing to launch the sale of a second set of NFTs advertised as “Embers,” which was anticipated to generate approximately \$1.5 million in cryptocurrency proceeds.

Frosties victims - Analysis & Identifications

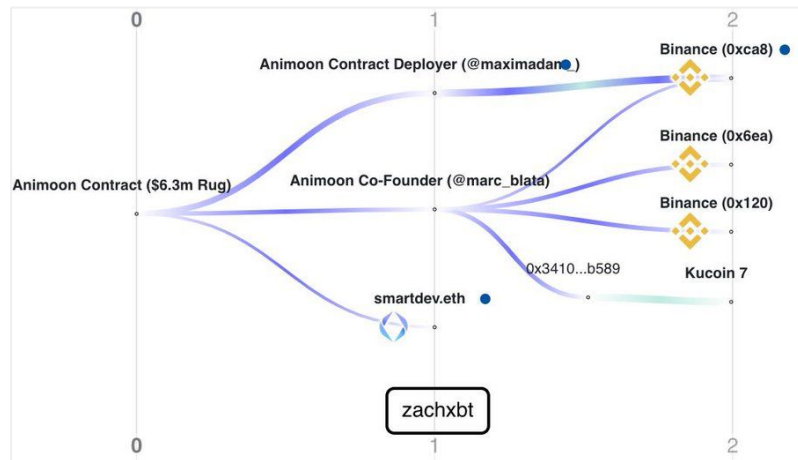
- **Why** are we doing that?
 - Help law enforcement identify victims.
 - Help lawyers with class actions.
- **What** are we looking for?
 - Any **point of contact**
 - Twitter, Reddit, Github, Mail, etc.
 - Timezone/Location information
 - Language
 - Usage of exchange with KYC/AML



Rug-Pull Victims Identification Animoon

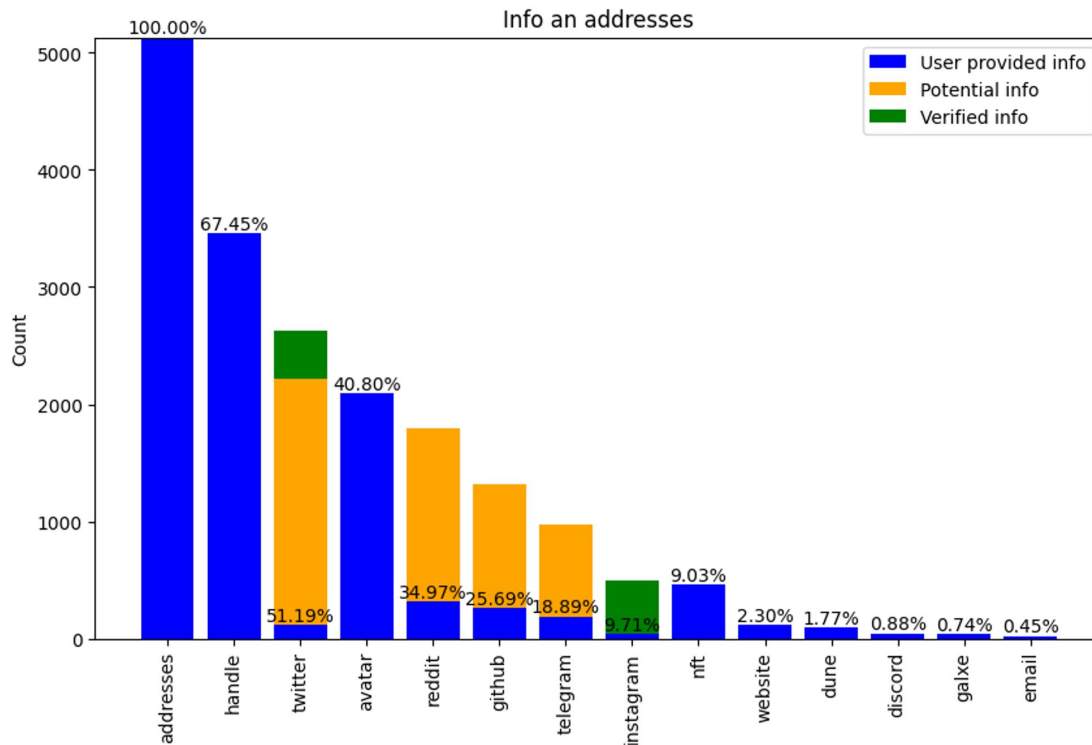
What is Animoon? \$6.3M NFT Rug-Pull

- Classic PFP NFT project
 - [Website](#), [Opensea](#), [Instagram](#)
 - **Advertised as a P2E game**
 - with utilities such as large giveaways
 - breeding, IRL trips, & more.
 - Claims to
 - Have an NDA signed with Pokémon
 - Be working with Bandai Namco (Digimon)
 - Promoted by Jake Paul
- Created by
 - **Marc Blata** ([@marc_blata](#))
 - Real name: Singainy Marc Oceane
 - Maxime Adam ([@MaximAdam](#))
 - Real name: Mounis Mokaddem
- Source: ZachXBT Analysis - [link](#)



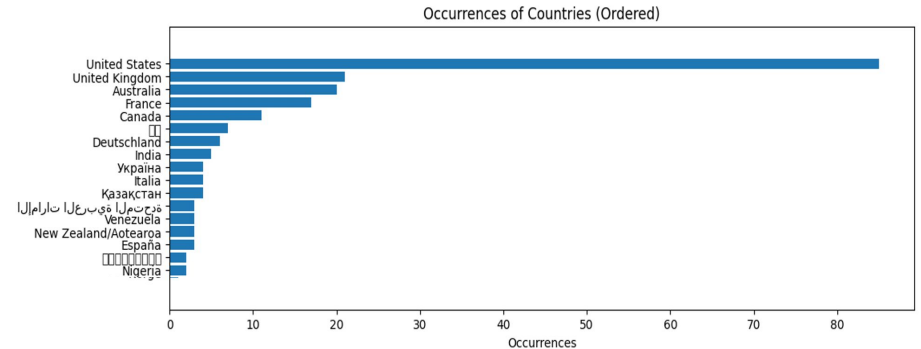
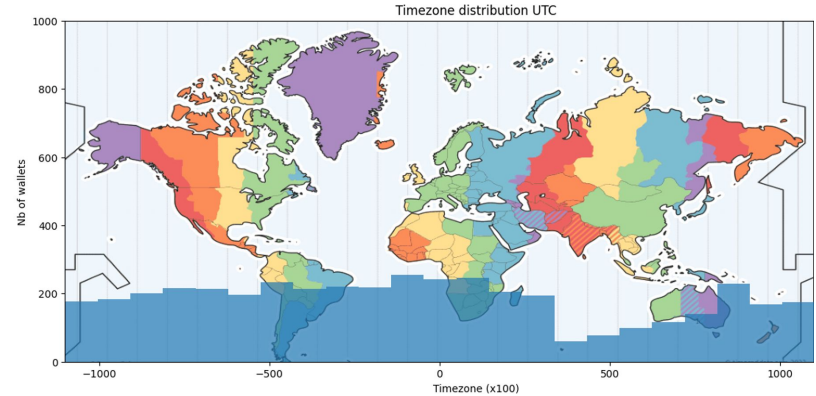
Animoon victims - Analysis & Identifications

- **Verified** information
 - Information verified by a website (ex: **OpenSea**, Galxe)
- **User-provided** information
 - Information provided by the user but not verified (ex: **ENS**)
- **Potential** Information
 - Other information found using Osint tools on handles related to the address (ex: **Maigret**)



How to detect Timezone/Location?

- **On-chain**
 - Transactions timestamps
 - NFTs with location information (POAP, etc.)
- **Off-chain**
 - Twitter description location & language
 - OpenSea bio language



What French victims should do?

- We identify:
 - ~ **20 french** & ~ 50 french speaking victims

- **Contacts**

- [Tweet](#)
- [Tweet #2](#)

ZIEGLER & ASSOCIÉS
@ZieglerAssociés

Le cabinet entame un recours concernant la soupçonnée arnaque d'ANIMOON. Si vous avez investi et n'avait eu aucun retour, contactez le cabinet ! Participez au recours : bit.ly/3xunBi6
[#animoon](#) [#nft](#) [#crypto](#)

Translate Tweet

Recours NFT

Récemment, le projet ANIMOON - qui a réussi à regrouper plus de 5 000 investisseurs pour un montant total levé de 6,3 millions de dollars est soupçonné d'être une arnaque.

Promettant des gains et avantages très importants aux premiers investisseurs & ce jour près de 3 mois après la vente des NFTs, aucun de ses engagements n'a été délivré.

Recours NFT

Si vous avez investi dans ce projet et avez été victime des messages et manipulations des fondateurs du projet mais aussi des influenceurs ayant fait sa promotion, il est temps de faire valoir vos droits.

www.ziegler-associés.com/recours-collectif-nft

6:28 PM · Jun 17, 2022

Collectif AVI
@collectifAVI

#CommuniquédePresse du #collectifAVI : Des #influenceurs de la télé réalité, dont #marcblata, visés par une plainte pour escroquerie en bande organisée. Une conférence de presse sera organisée avec le cabinet @ZieglerAssociés le 23 janvier à Paris. bit.ly/3iwyA78

Translate Tweet

COMMUNIQUÉ DE PRESSE DU COLLECTIF AVI
Paris, le 12 janvier 2023

Pour la première fois en France, des victimes, accompagnées par une association et un cabinet d'avocats, mettent des "influenceurs" de télé réalité face aux conséquences juridiques de leurs actes : une plainte pour escroquerie en bande organisée sera déposée prochainement à Paris.

Une conférence de presse est organisée afin de vous informer sur cet événement le 23 janvier 2023 à 9h00, à l'Espace Hamelin, Salle du Conseil 17 rue de l'Amiral Hamelin, 75116 Paris en présence de représentants du Collectif AVI et du cabinet Ziegler & Associés.

Pour la première fois en France, des victimes, accompagnées par une association et un cabinet d'avocats, mettent des "influenceurs" de télé réalité face aux conséquences juridiques de leurs actes : une plainte pour escroquerie en bande organisée sera prochainement déposée à Paris.

Une conférence de presse est organisée sur cet événement le 23 janvier 2023 à 9h00 à l'Espace Hamelin Salle du Conseil 17 rue de l'Amiral Hamelin 75116 Paris en présence de représentants du Collectif AVI et du cabinet Ziegler & Associés.

CONTACT COLLECTIF AVI
collectif@avi.com contact@collectifavi.com
twitter : @collectifAVI instagram : collectifavi linkedin : collectifavi facebook : avicollectif

1:27 PM · Jan 12, 2023 · 189K Views

Use-cases

Tornado Cash

User Statistics & Deanononymization

What is Tornado Cash ?

- **Tornado Cash**

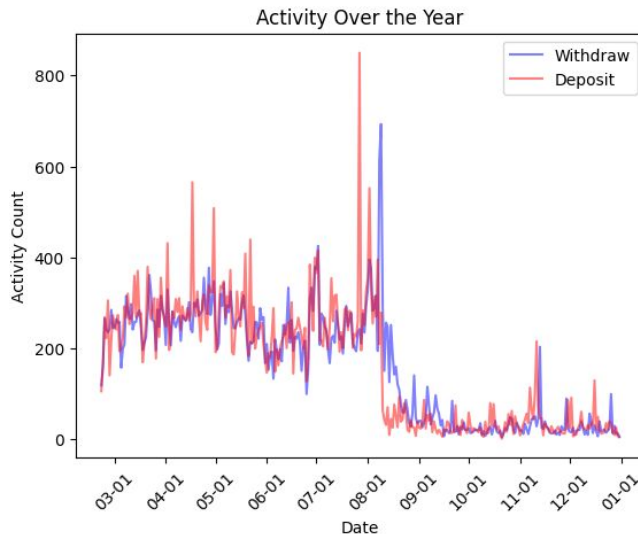
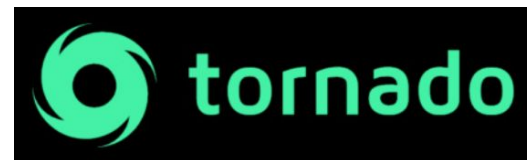
- Open source, non-custodial
- Fully decentralized **cryptocurrency tumbler/mixing service**
- Running on EVM-compatible networks
- Designed to make it harder to trace cryptocurrency transactions.
- Used worldwide as a **money-laundering** platform.



- **In August of 2022**

- the U.S. Treasury's Office of Foreign Assets Control (OFAC) **sanctioned** Tornado Cash.
- Blacklisted the service, making it **illegal for US citizens, residents, and companies** to use.

- **How many Americans used Tornado Cash in 2022?**



How does Tornado Cash work?

- Processus

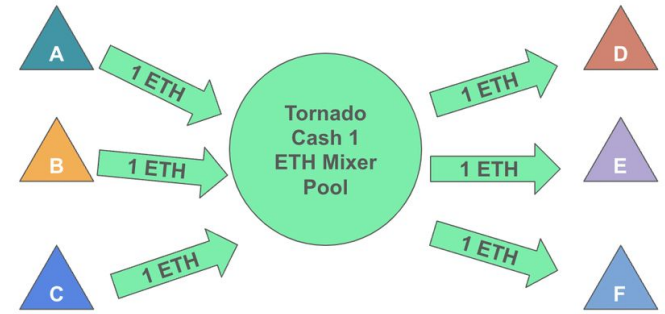
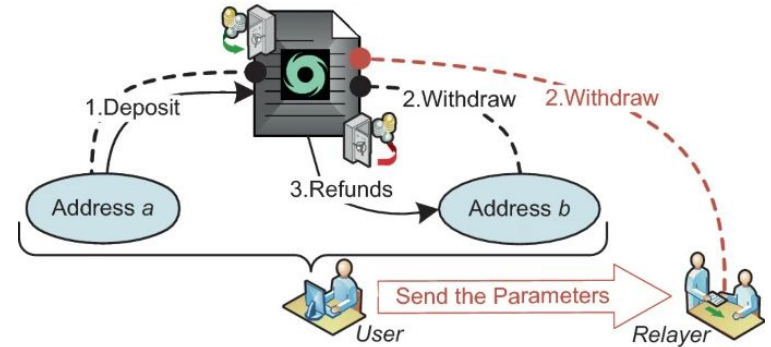
- **Depositor** (A) sends ETH to Tornado Cash pool
 - Fixed values per pool: 0.1, 1, 10, 100 ETH
 - Generate a random key: note
- **Wait** some time to improve the privacy
- A user (address B or a Relayer) **withdraw**
 - Provide proof of the note
- Money is sent to the **Receiver**

- Different actors

- **Depositor**: send the money
- **Withdrawer**:
 - **Relayer**: withdraw for someone else
 - **Receiver**: receive the money

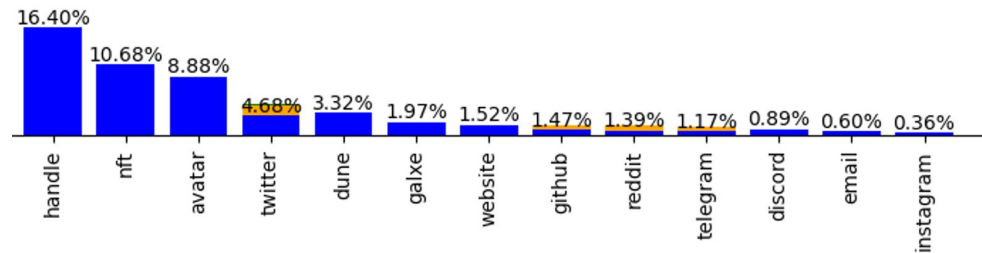
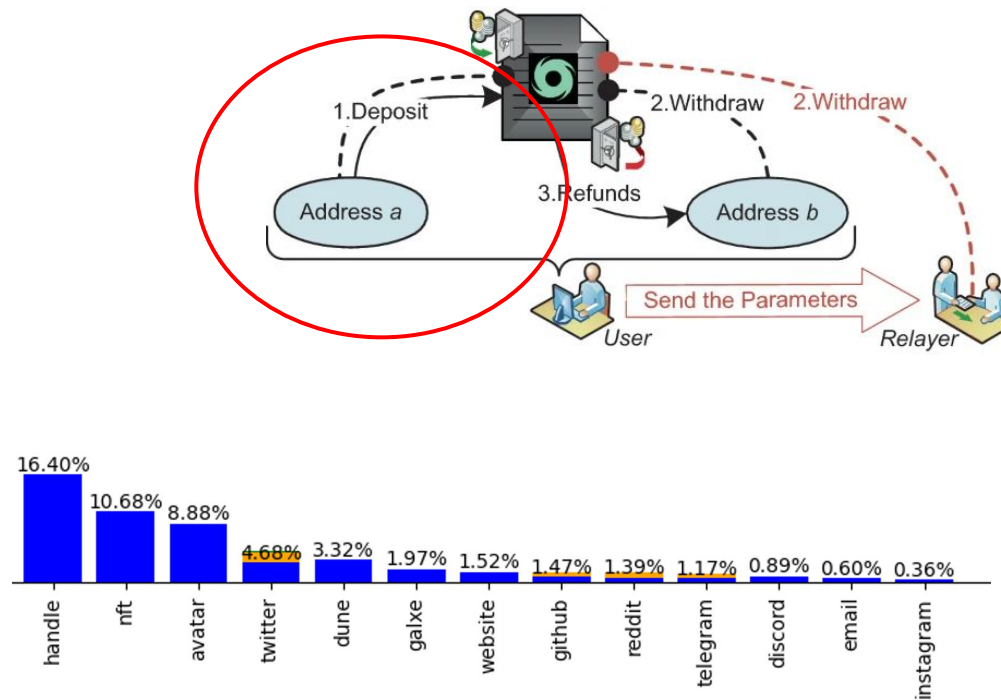
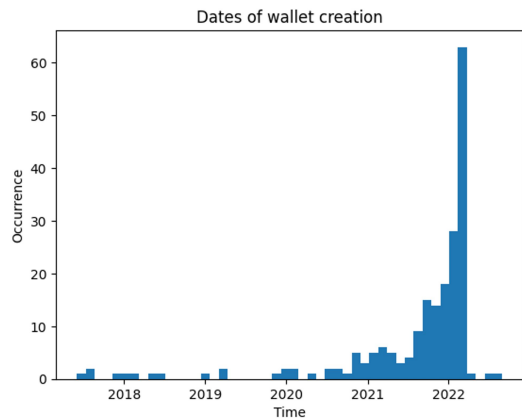
- Sources:

- What is a cryptocurrency mixer and how does it work? - [link](#)
- How does Tornado Cash work? - [link](#)
- Analysis of Address Linkability in Tornado Cash on Ethereum - [link](#)



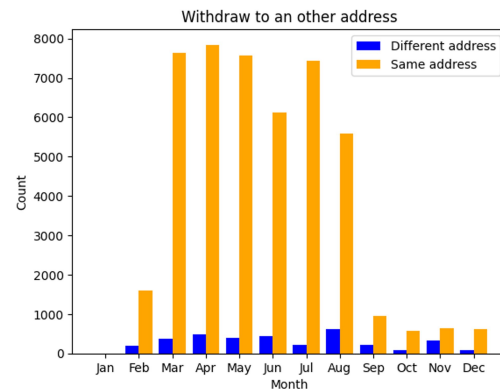
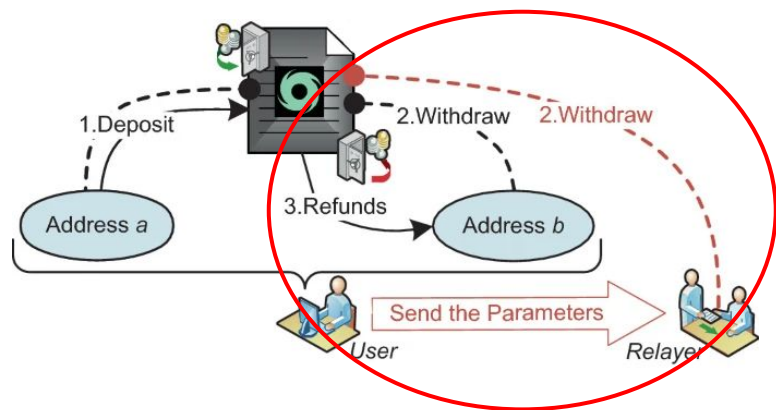
Depositor Statistics (Feb - Dec 2022)

- Global statistics
 - 50 687 transactions
 - **15 722 unique addresses**
- OSINT statistics
 - Most wallets < 1 year old
 - **~50 users** located in the USA



Withdrawer Statistics (Feb - Dec 2022)

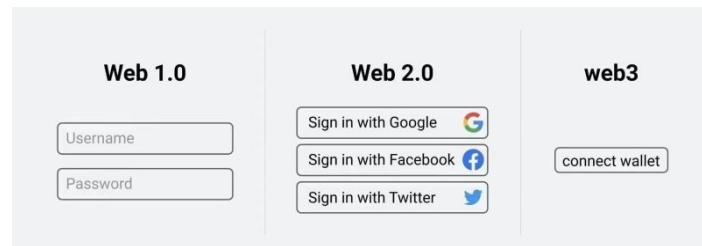
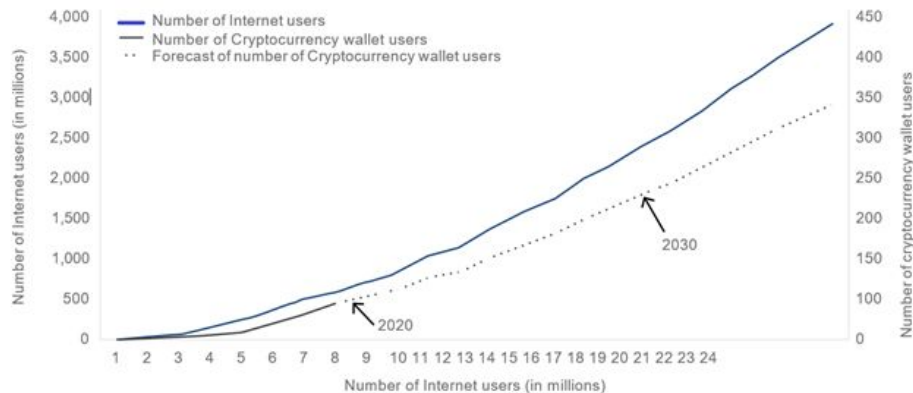
- Global statistics
 - 50 024 transactions
 - **1 444 unique addresses**
- **Same** Withdrawer & Receiver
 - Already have ETH to spend to initiate withdrawing
 - I.e. Already funded address
- **Different** Withdrawer & Receiver
 - No need for any money in the wallet to pay the transaction fees
 - The Relayer takes a cut on the retrieved ETH
 - Meaning a brand-**new wallet can be directly funded with Tornado**
- OSINT statistics
 - Recipient:
 - 20k + recipients
 - Relayer:
 - 257 relayers



Conclusion & Future

Conclusion & Future

- Takeaways
 - **Blockchain OSINT is fun and surprising**
 - Accessible with only public tools
 - A good start to discover how blockchains work
 - Mandatory to control your OPSEC
- How blockchains will evolve in the future?
 - **Better adoption** and native integration
 - More day-to-day users
 - **Privacy-Oriented Blockchain** L1/L2
 - Leveraging on ZKP (zero-knowledge proof)
 - [Ethereum ERC-5564](#): Stealth Addresses
- What are Fuzzinglab's next steps?
 - Continued building our **web3 deanonymization product**
 - More talks, training & workshops
- Sources: Cryptocurrency Adoption Across Europe and America 2021 - [link](#)



Thanks for your time! Any questions?

- Thanks to
 - **LeHack** staff, **Sylvain**, **OSINT-FR**, **Fuzzinglabs** team, etc.

Patrick



Tanguy



- Twitter: [@Pat_Ventuzelo](https://twitter.com/Pat_Ventuzelo)
- Mail: patrick@fuzzinglabs.com