vicomtech

MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Entity identification in the cryptoasset ecosystem

International Digital Security Forum 2022

Anti-FinTer

Context

TITANIUM: Tools for the Investigation of Transactions in Underground Markets

Versatile artificial intelligence investigative technologies for revealing online cross-border financing activities of terrorism

Context

Entity: person or organization that controls or can control multiple public-key addresses

TITANIUM: Tools for the Investigation of Transactions in Underground Markets

Versatile artificial intelligence investigative technologies for revealing online cross-border financing activities of terrorism

Context

TITANIUM: Tools for the Investigation of Transactions in Underground Markets

Versatile artificial intelligence investigative technologies for revealing online cross-border financing activities of terrorism

Entity: person or organization that controls or can control multiple public-key addresses

Why is important to identify entities?

- During an investigation, it is not enough to detect malicious/illicit addresses or transactions.

- LEAs need to investigate the entity that has generated these malicious/illicit activities

Context

TITANIUM: Tools for the Investigation of Transactions in Underground Markets

Versatile artificial intelligence investigative technologies for revealing online cross-border financing activities of terrorism

Entity: person or organization that controls or can control multiple public-key addresses

Why is important to identify entities?

- During an investigation, it is not enough to detect malicious/illicit addresses or transactions.

- LEAs need to investigate the entity that has generated these malicious/illicit activities

However, LEAs have difficulty to start an investigation:

- A large number of addresses to be controlled (waste of time and resources)

- Unknow *real-world* actor's identity

Entity Taxonomy*

- **Miner:** who participates in validating transactions on the blockchain
- **Service:** A service refers to some software functionality or a set of software functionalities that can be used by different actors for different purposes.
- **Exchange:** that provides services to buy and sell tokens and for exchange of FIAT currencies

- **Trading platform:** P2P Exchange, Decentralized Exchange
- **Wallet providers:** Hardware wallet, software wallet, custodian wallet
- **Escrow:** a contractual arrangement in which a third party receives and disburses assets
- **Tumbler:** a method of scrambling or anonymizing the source of one's cryptocurrencies
- **Darknet Market:** is a commercial website on the web that operates vias darknets

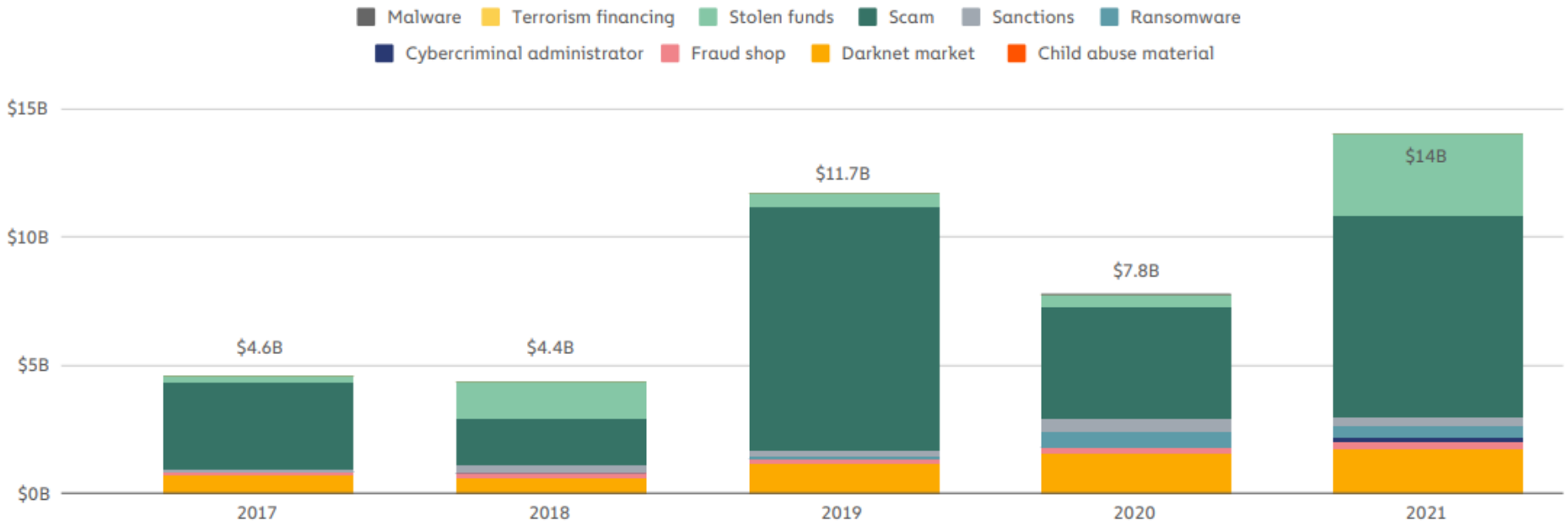
Other: Gambling, Flash Loan, Crypto ATM, Dead drop, etc.

**Entity Taxonomy: version 0.3, Last Modified: 2022-01-21, Creator: INTERPOL Darkweb and Virtual Assets Working Group*

Cryptoasset ecosystem

Cryptocurrency-based crime hit a new all-time high in 2021, with illicit addresses receiving $14 billion over the course of the year, up from $7.8 billion in 2020.

Total cryptocurrency value received by illicit addresses | 2017–2021

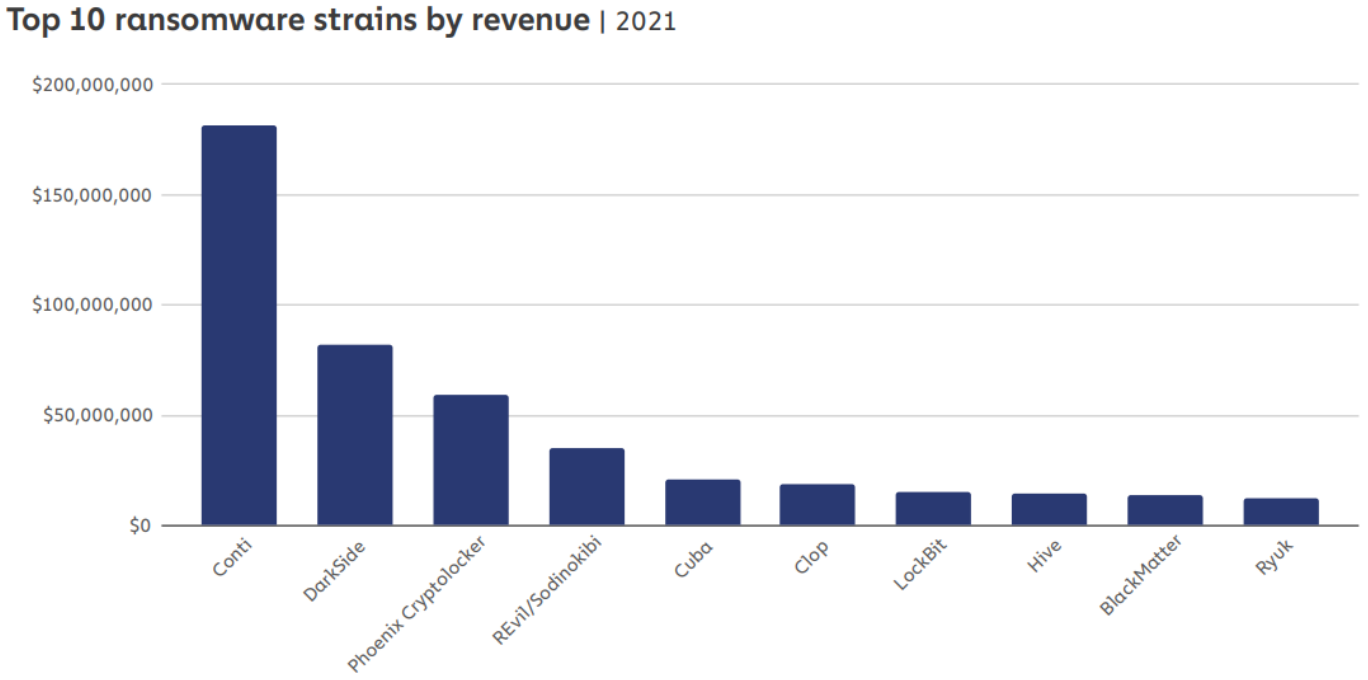


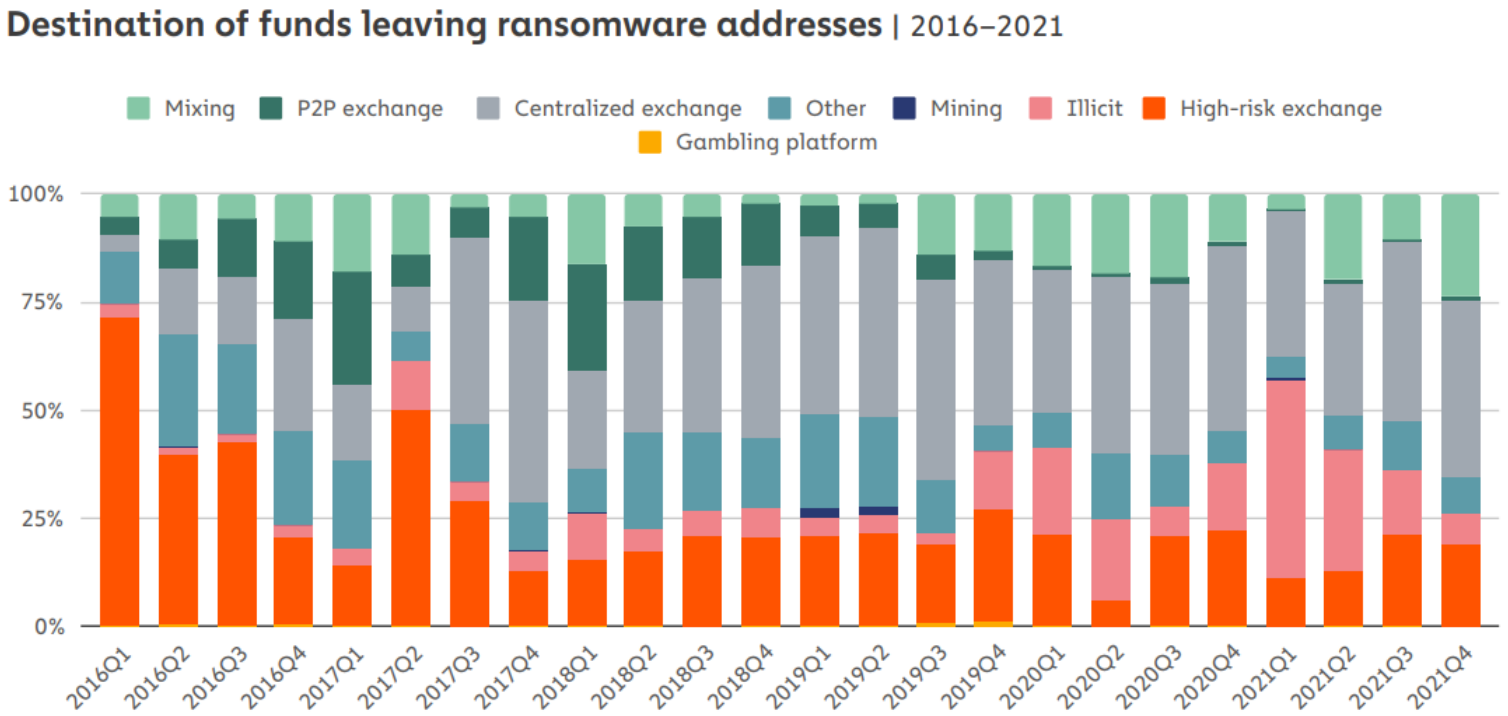
*Source: Crypto-Crime-Report-2022

Cryptoasset ecosystem

Ransomware

In 2020, $ 692 million were involved in ransomware payments and about $602 million worth in 2021.
Most ransomware strains have laundered their stolen funds by sending them to centralized exchanges.



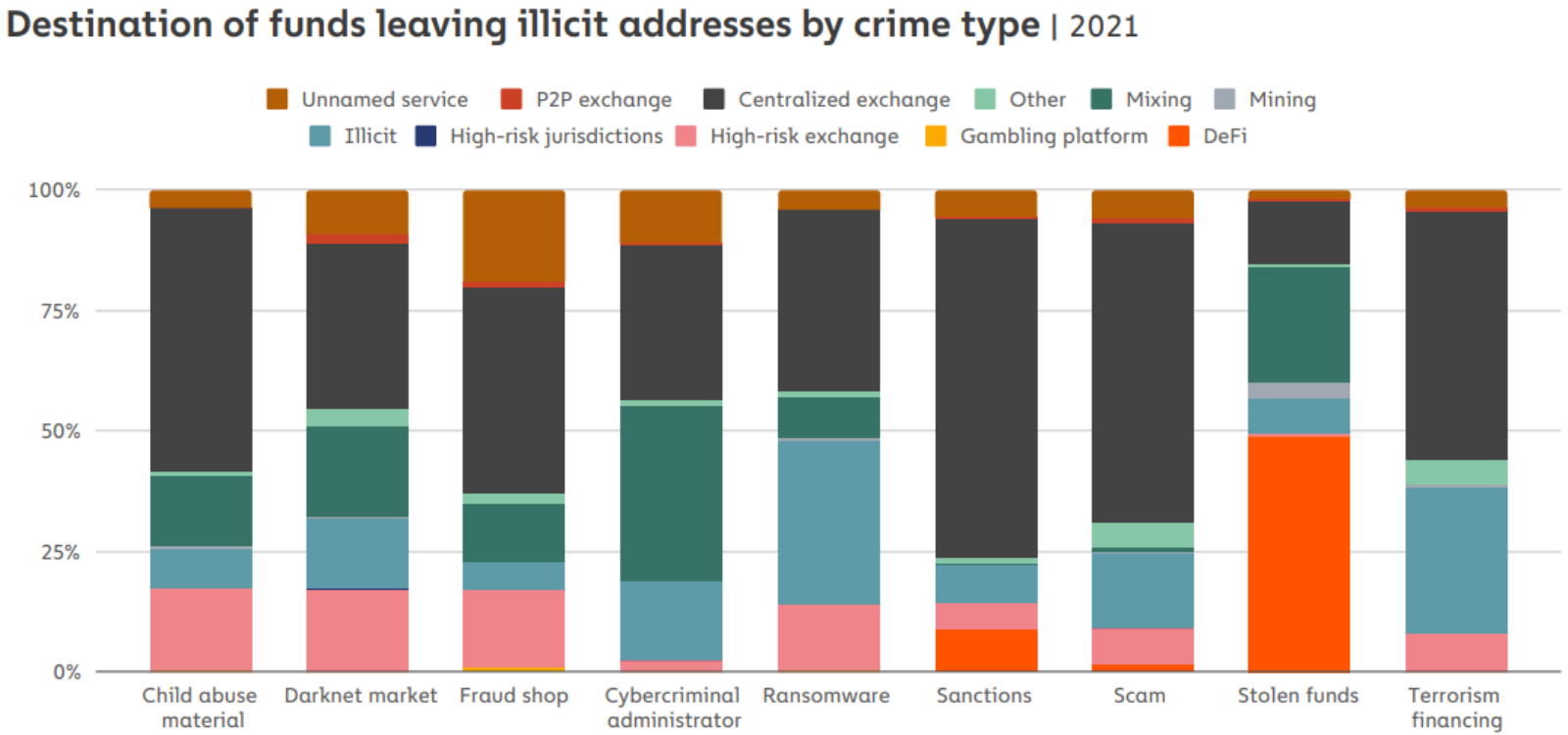


Source: Crypto-Crime-Report-2022

Cryptoasset ecosystem

Money laundering

While billions of dollars worth of cryptocurrency move from illicit addresses every year, most of it ends up at a surprisingly small group of services, many of which appear purpose-built for money laundering based on their transaction histories.



*Source: Crypto-Crime-Report-2022

Cryptoasset ecosystem

Terrorism Financing (TF)

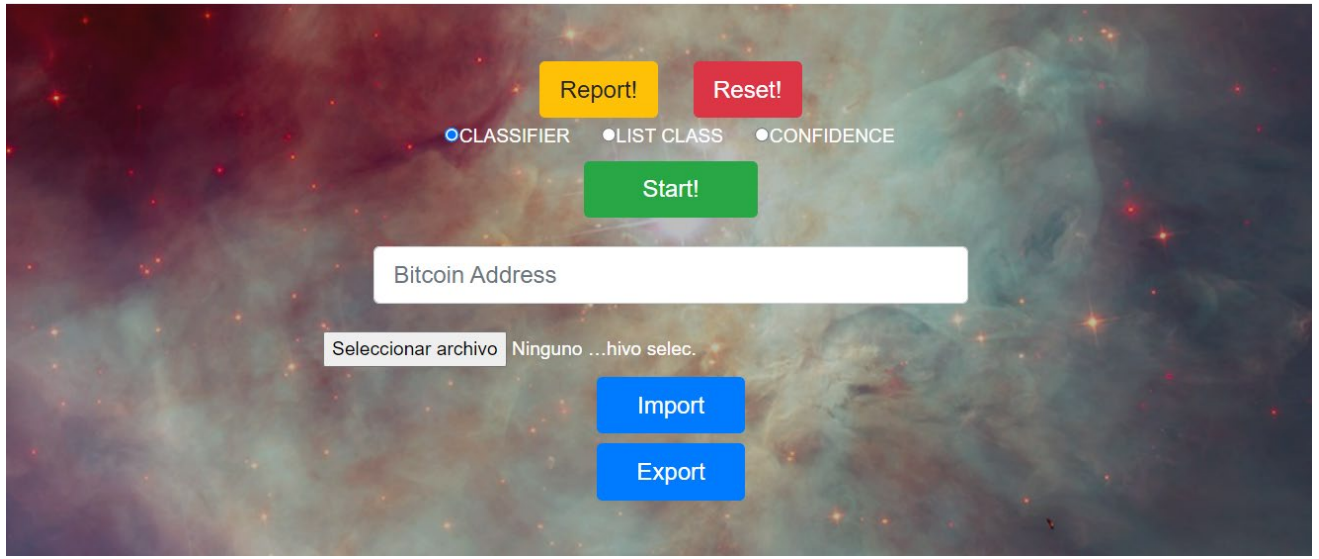
In 2019 and 2020, al-Qaeda raised cryptocurrency through Telegram channels and Facebook groups. More than $1 million was seized from a money service business (MSBs) operator who facilitated some of these transactions.

In the early Spring of 2021, al-Qassam Brigades, Hamas' military wing, collected more than $100,000 in donations. In July, the Israeli government seized much of it from associated MSBs.

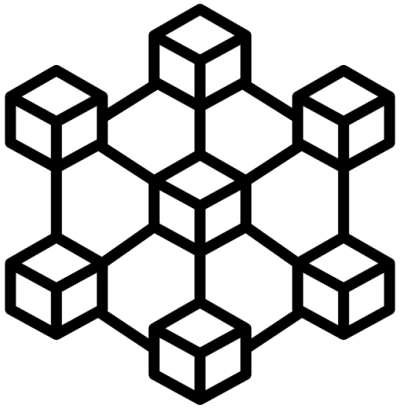
!! However, it is difficult to relate TF directly with crypto entities !!

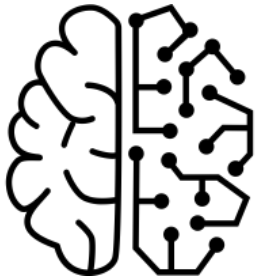
**Source: Crypto-Crime-Report-2022*

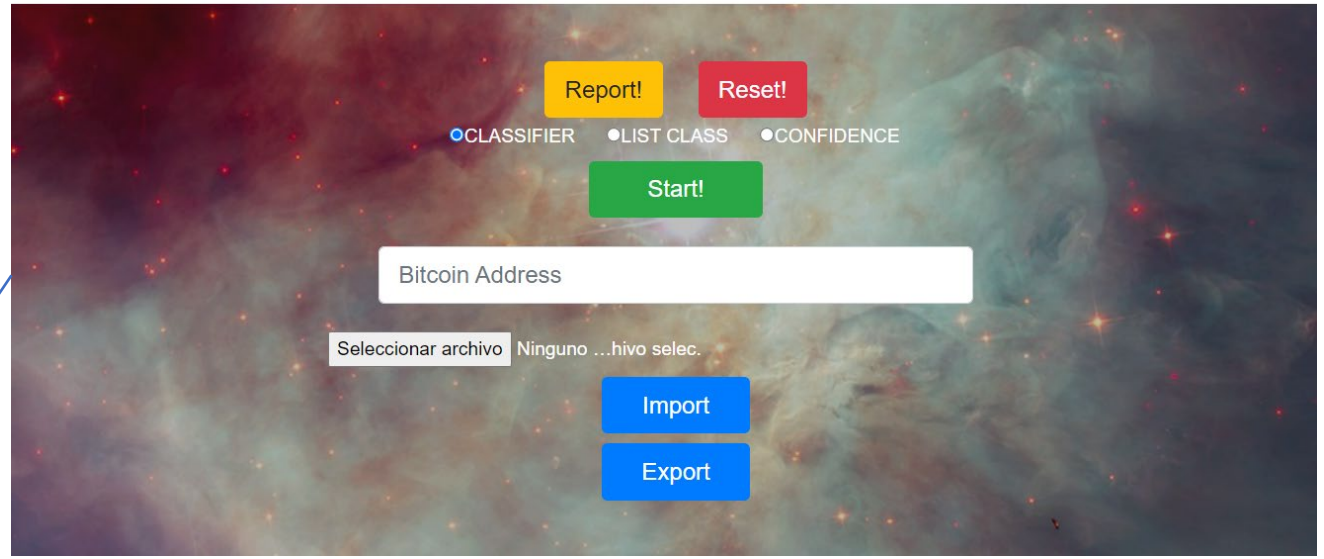
OdainSare


Report!
Reset!
CLASSIFIER
LIST CLASS
CONFIDENCE
Start!
Bitcoin Address
Seleccionar archivo
Ninguno ...hivo selec.
Import
Export

OdainSare



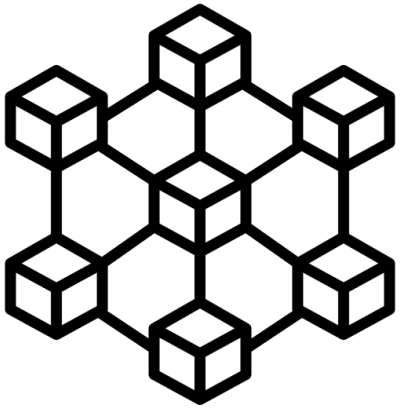


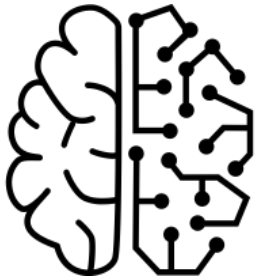

Report!
Reset!
CLASSIFIER
LIST CLASS
CONFIDENCE
Start!
Bitcoin Address
Seleccionar archivo
Ninguno ...hivo selec.
Import
Export

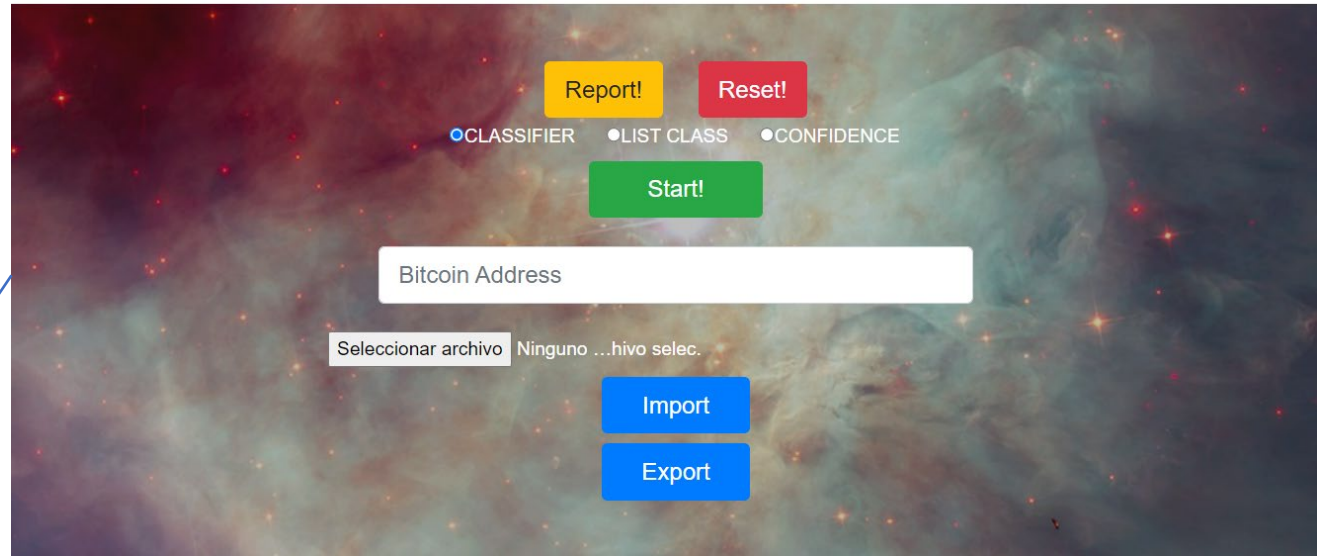
Anti-FinTer

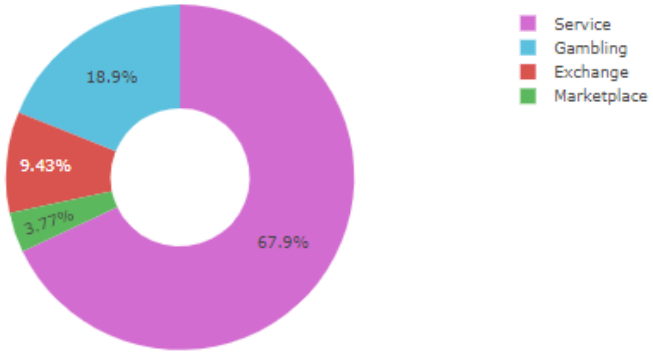
vicomtech
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

OdainSare









Address: 16tSmKHUR4K3EV82txfDy5dgn3mxKT2UJW

Cluster Label: Poloniex.com

version: 1

Open challenges

- How we can prevent terrorism financing since they can also use licit funds?

- We the introduction of technology such as Non-fungible Tokens (NFT), how do entity behaviours change? Does it promote new illicit patterns?

- How is it possible to deal with the (grown) number of darknet markets?