Department of business and management

Management and Computer Science

Academic Year 2021/2022

Money Laundering in the decentralized era: how Blockchain technology enables illicit activities

Supervisor:

Dr. Gianluigi Me

Candidate:

Francesco Di Stefano

INDEX

INTRODUCTION

1.1 Why this subject?

I decided together with my supervisor to tackle this topic for many reasons, the first is: because with the exponential growth of the NFTs market many new users are being involved in this world but almost the majority of them do not even take it into consideration the potential criminal issues that this new technology can enable.

Furthermore, I have always been attracted to cybercrime themes because, in my opinion, this kind of job has an effective and tangible effect on the real world. Really gives me the idea to work on something that really helps the community and then all the parties in the network gain an effective benefit from this kind of duty.

Professor Gianluigi Me suggested this thesis to me mainly for the Internet Organised Crime Threat Assessment (IOCTA) 2021written by Europol. In this paper are covered the most popular online criminal trends and practices, one of the most recurrent is money laundering. The professor assigned to me this work also because these are themes that will surely be present and important in the future too, considering that nowadays these topics have a very dark nuance for many insiders and as we will see also for the institutions.

1.2 Research questions

The main objective of the research is to describe how money laundering works throughout NFTs and to use the Maltego platform in order to derive an investigation method aimed to find money laundering evidence and to drive some conclusions about the modalities of this illicit activity. This thesis will also highlight the volume of this phenomenon and explain what is the impact of NFTs money laundering in the crypto-economy. The paper will also describe how authorities can investigate such crimes and if these methods are effective.

In order to answer these questions and to clarify the arguments, an introduction to Blockchain and NFT will be given, also covering some legal aspects such as the difference between trade wash and money laundering. Furthermore, AML (anti-money laundering) rules and protocols will be also depicted.

1.3 Overview of the tools and sources for the analysis

Since this argument came up very recently it was not covered by any of the courses I attended during my bachelor's degree so I had no material on my own. My supervisor provided me with some hints regarding the tools and the material to retrieve. The Maltego platform, suggested by the professor, aims to empower investigators with a specific and efficient tool that allows real-time data mining and data representation in order to identify patterns and connections; and by this definition, we can call that an open source intelligence (OSINT) tool. OSINT is a discipline of intelligence that deals with the research, collection, and analysis of data and news of public interest collected from open sources. The tool is written in java and runs on all the major operating systems: Windows, Linux, and Mac. For a deeper comprehension of how Maltego works I will now explain shortly how this tool gathers data; first of all this tool has two reconnaissance methods: infrastructural and personal. The first deals with the internet domain as a matter of fact covers DNS information, mail exchangers, zone transfer tables, DNS to IP mapping, and related information. The second includes personal information such as email addresses, phone numbers, social networking profiles, mutual friend connections, and so on. The Maltego client sends an XML file containing data to a server through an HTTPS connection, after processing the results are sent back to the client. Maltego has three main versions: Pro, Enterprise, and Community each one of these has different features and capabilities, for this project I adopted the community edition.

For other purposes, I also consulted some papers from Chainanalysis the most important platform involved in the Blockchain investigations

I also used RapidMiner for a quick analysis of a dataset. RapidMiner is an application that can be used for some exploratory data analysis, we saw this tool also during the course taught by my advisor.

1.4 What is money laundering

By money laundering, we mean a whole criminal process aimed to reintroduce back into the market money that comes from illegal activities, for example, extortion, drug sales, and illegal gambling.

Generally, this process involves three steps: placement, layering, and integration; the first concerns the introduction of cash into the financial system by some means, and the second step is made in order to camouflage the illegal source of the cash by performing complex transactions, the last one is the acquisition of the "clean money".

The United Nations Office on Drugs and Crime (UNODC) has estimated that the global amount of money laundered per year is between the 2% and 5% of the global GDP, the values are not easy to retrieve since the clandestine nature of this process. There are other statistics that can give us an idea of how much the phenomenon of money laundering is growing in the last period: The average global money laundering risk score – as reported by the annual Basel AML Index - saw an increase in 2021 from 5.22 to 5.3 (out of a maximum score of 10), 22.0% of money laundering offenses in the US in 2020 involved loss amounts greater than $1.5 million, the median amount of money laundered in the US in 2020 was $301,606 and 90 percent of the money laundered goes undetected.

Money laundering affects the economic system for another reason, that is, it cancels out trust in financial institutions and it is well-known that integrity is one of the most valuable assets in the financial field.
If we imagine, for example, that a huge amount of money was laundered by a major bank and then the police discover that crime, most customers and financial partners could begin to cut all economic relationships with this bank, hence causing big losses and potentially starting a domino effect to all stakeholders.

In order to prevent this criminal activity, all financial institutions have to comply with the AML regulation which involves a set of mandatory procedures. Europe is constantly updated regarding anti-money laundering laws, the latest directive approved (end of 2020) aims to broaden the scope of existing legislation and tighten criminal sanctions to enable financial institutions and authorities to do more in the fight against money laundering and terrorist financing. Anti-Money Laundering Directive VI increases the number of offenses that fall within the definition of money laundering and provides a unified list of 22 offenses, which are assumptions that constitute money laundering including some tax offenses, environmental crimes, and, for the first

time in an EU Directive on money laundering, money laundering, cybercrime offenses. It is possible to sum up the VI directive in six points :

1. Unified list of offenses which now include cybercrime and environmental crime;
2. Additional money laundering offenses: supporting and aiding, attempting and inciting;
3. Extension of criminal liability to legal persons;
4. Increased international cooperation for the prosecution of money laundering;
5. Harder punishments;
6. Double criminality requirement for 6 specific offenses:
    - organized criminal association and racketeering;
    - terrorism;
    - trafficking in human beings and smuggling of migrants;
    - sexual exploitation (including children);
    - illicit trafficking in narcotic drugs and psychotropic substances;
    - corruption

1.5 History of money laundering in the fine art sector

There has always been a link between money laundering and the fine art sector even before the advent of digital art, for this motivation it seems to me necessary to talk about this phenomenon to better understand how these illegal practices can become even more hidden and efficient exploiting the Blockchain.

The latest available estimates provided by The United Nations Office on Drugs and Crime (UNODC) reveal that about 3 billion dollars are laundered throughout the fine art market every year; this is due to: the anonymity of the parts involved in the transaction and price flexibility, a lack of authorized regulatory oversight regarding the process of art valuation, the pricing of art is a highly subjective practice that can allow criminals to launder huge sums of money in particular through art auctions.

Most of the time the transaction happens in the so called *free ports* which are a sort of warehouse but with no specific legislation, indeed all the goods kept in this specific case are defined as *in transit* so no specific law is applicable even taxes are absent. Even if this type of crime is very hard to detect, now I will discuss 2 examples.

The first one involved 47 paintings, some of which were painted by Renoir, Picasso, and Salvador Dalí. All these works of art were found in Philadelphia in the home of Ronald Belciano, a well-known drug dealer, who used this method to launder money from his criminal business. In 2015, he was sentenced to more than five years in prison for dealing drugs and for laundering illicit proceeds by taking advantage of one of the art market's signatures features as reported by the New York Times article.

The second example is the story of the famous painting "Hannibal" by Jean-Michel Basquiat. In 2006 the Brazilian banker and financier Edemar Cid Ferreira was sentenced for 21 years of prison for bank fraud, tax evasion, and money laundering. The painting was smuggled by Ferreira to the US from Brazil, via The Netherlands with false invoices stating that the masterpiece was worth 100$ while the real value is about 8 million dollars.

For what concerns AML regulation in this sector there is not a unique protocol but the EU, USA, and the UK follow different regulations although these are very similar to each other. In the US the latest law that covers this argument is the Anti-Money Laundering Act of 2020 (AMLA 2020) which was written to be broad enough to include in the definition of financial institutions,

not only the antiquities dealers themselves but also the intermediaries involved in the sale and purchase of such items. And as financial institutions, all the market participants must comply with the *Customer Due Diligence* requirements for financial institutions (CDD Rule) which has 3 main points:

1. Ascertain and verify the identities of customers and ultimate beneficial owners;
2. understand the nature and purpose of customer relationships to develop customer risk profiles;
3. conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, maintain and update customer information.

In the EU the current regulation is the 6th Anti-Money Laundering Directive which amends the 5AMLD that was aimed to increase transparency in this sector. The latest directive has made the verification of the parties mandatory if the transaction is over 10 000 €, in addition, this law has made Anti-Money Laundering (AML) and Customer Due Diligence (CDD), for all the participants in the art market, compulsory.

BLOCKCHAIN AND NFTs FUNDAMENTALS

2.1 The basic mechanisms of Blockchain technology

In order to better understand what are NFTs and how they work, it is fundamental to have a glance at the technology they rely on, the Blockchain. Basically, the blockchain is nothing more than an electronic ledger distributed among the nodes of the network, so every node of the network has the same copy of the ledger which is composed of records called blocks. Each block is linked to the other and secured by some kind of cryptographic function. Since every block is linked to the other it is impossible to alter the state of a block without interacting with the previous and the successor, this feature enables the irreversibility of every transaction carried out using this system.

The main purpose of the blockchain technology is to reduce, in theory, centralization in the network putting all nodes on the same level and keeping track of every movement in the network in an extremely secure and accurate way.

There is not a unique type of blockchain, these can differ: in the choice of the algorithm that validates the transaction, in the way of encrypting the blocks, in public or private, and in the language in which they are written; but the common feature is that the participants, or at least a part of them, has to approve every transaction in the network. For public blockchain we mean a network in which every node, in theory, has the same rights and there is no supervision; everybody can join the blockchain, in this type of network always appear a crypto economy with a native currency. For private blockchain we mean a network controlled by an authority that selects and approves the nodes that will have to validate transactions, clearly is more efficient and secure than the public one; it is also fair to mention that there exist hybrid solutions too.

It must be clear that even if all transactions are public the real identities of the parties are not, indeed anonymity is one of the main features of this technology. Blockchain enthusiasts are prospecting a new form of the web called “Web 3”, a network in which exist only decentralized applications relied on the blockchain and in which the tech giants do not hold the majority of data, which is the actual “Web 2”. The data decentralization means decentralization of power and thus Web 3 would be safer since no one would have more power than the other. This new model of the web would be built on crypto economy that empowers smart contracts and thus DAPPs.

It is important to remark that this kind of technology suffers from some issues, and a lot of experts think that Web 3.0 is impossible to implement. First of all, we must consider that the Blockchain technology requires some know-how from the users so the vast majority of internet people are reluctant to study more technical features for having almost the same functionalities. The real challenges are the technical ones this kind of technology suffers from: scalability, interoperability, inefficiency, and energy consumption problems. The scalability problem is related to the number of nodes that join the network in simple words, the more people or nodes join the network, the chances of slowing down is more, but there are already many solutions to this problem such as the "Sharding" which I will discuss in a while or to do transactions off-blockchain and only use blockchain to store and access information, but even with these solutions centralized systems light-years faster. Every single blockchain uses different methods and architecture to reach the same goal, this leads to interoperability issues where these chains are not able to communicate effectively; the issue also persists when it comes to traditional systems and systems using blockchain technology. This kind of network is inefficient since it requires a lot of memory and computational power for every node to run, this is due to their complexity and their encrypted, distributed nature, blockchain blockchains can be slow and cumbersome, and transactions can take a while to process; also here there are some solution such as "Lightning networks", which is a second layer network that allows multiple off-chain transactions. Blockchain technology is not eco-friendly, every time the ledger is updated with a new transaction the miners need to solve the problems which means spending a lot of energy. However, not all blockchain solutions work in the same manner permissioned systems are more efficient in this sense.

In conclusion, we must take into account that in a decentralized web there is not a central authority who can control illicit activities in a sense criminals would be better of with the adoption of Web 3 and blockchain.

Centralized institutions, tech giants, and banks initially were distant from such reality then something changed, at least for some of them. Apple is still reluctant to embrace this technology, Microsoft instead has implemented a blockchain-based tool called "Azure Blockchain Service", which allows users to create their own consortium networks and applications using prebuilt networks and software. For the banks there is a different situation since, in theory, Blockchain could be the killer application for them so to not be overwhelmed by the progress banks are starting to invest and study the possible applications of this new technology.

The first decentralized blockchain was Bitcoin designed by Satoshi Nakamoto in 2008 the main purpose was to move value without any trusted central authority in a peer-to-peer network. In Bitcoin transactions are validated by the so-called “miners” who are nodes in charge of solving computationally intensive problems that make secure the transaction; every time a miner solves a transaction gets a reward and a fee, and the last one is paid by the parties of the transaction. The process of resolving problems, the solution is to find a double hash that is lower than a given target, is called *proof of work* that was implemented to solve the double spending problem, create consensus and make it almost impossible for any hacker to attack the system. By double spending problem we mean the situation in which the same single token can be spent more than once. This problem is assessed by the amount of time required to validate the transaction, which is 10 minutes, and also by the fact that the transaction is also checked by other nodes after the miners approve it. In order to prevent inflation the creators of Bitcoin set a maximum cap of 21 000 000, when this number of bitcoins will be reached miners will take only fees for validating transactions.

The other colossus of the blockchain technology is Ethereum on which I will spend more time since NFTs are based on this type of electronic distributed ledger. Ethereum is an open blockchain written in a touring complete language that uses proof of work as a validation method as well as bitcoin but to validate a block takes 12 seconds and especially Ethereum does not have a fixed cap of tokens. Miners only take fees from transactions that are paid from the sender in a unit of account called *Gas*; the amount of gas required is proportional to the amount of resources a node needs to use for validating the transaction. Currently, Ethereum 2.0 is under development; a new version that will adopt a new consensus algorithm, *proof of stake*, and will improve the number of transactions per second from about 15 up to tens of thousands, this is possible thanks to a scalable architecture called *sharding*. But why this change is needed? For three main reasons, the first is that the PoS is far more energy efficient than PoW and so it is cheaper and will need less computing power to validate a block, the second reason is that Ethereum 2 will be more scalable thanks to the sharding that I will explain later, and the last one is security because in the new version requires a minimum of 16 384 validators, making it much more decentralized. Now I will discuss briefly how PoS works and what is the sharding. PoS has a different way of selecting miners, as a matter of fact, they are selected in proportion to their quantity of holdings in the associated cryptocurrency, the higher the amount of tokens the higher the probability to validate a transaction, it is important to highlight that the number of tokens staked is not spendable anymore. Validators are randomly chosen to create blocks and are responsible for checking the blocks they don't create. A user stake is also used to incentivize correct behavior by

the validator. Sharding is a sort of horizontal blockchain partitioning; with sharding, Ethereum moves to a parallel execution model, in which nodes are assigned to process only certain computations. This will allow for multiple, parallel, transaction processing at the same time. But the reason why Ethereum became so popular is that this blockchain allows the application of smart contracts and NFTs exchanges. Smart contracts are basically computer programs that automatically execute an action legally relevant, they are written in solidity, and they enable decentralized applications (Dapps) what makes a Dapp different than a traditional app is that it's built on a decentralized network, like Ethereum. And now let’s move to NFTs.

2.2 NFTs and their role in the blockchain

NFT stands for “Non-Fungible Token” where *not fungible* means that they are not interchangeable or distinguishable; by definition, they are tradable financial goods stored in a blockchain. NFTs can be created by anyone since no programming skill is required and they can contain references to digital files such as pictures, videos, voice mails and etc; depending on the creator, buying an NFT can give you special benefits such as special access to an event or a discount on something. The possession of an NFT represents a proof of ownership but does not necessarily imply that the owner possesses IP right on the asset that the NFT represents.

One of the most famous application of NFTs is digital art. there are many examples of Non-Fungible Tokens that are priced and considered as fine art masterpieces; in this world it is very popular the *generative art*, a new type of art in which an autonomous system is involved in the creation process. Often this kind of art images are created by assembling simple pictures component in a different way. Many famous NFTs collections such as Bored Apes and EtherRocks belong to this style.

The most expensive one is called “Merge” created by Pak purchased for 91.8 million dollars, There are also many artists that are starting or already have an NFT collection, Lee Mullican, Linda Dounia are some of them. But why the NFT market is attracting so many artists? The answer is very simple thanks to blockchain the art market sector is expanding also in the digital format and this is a huge chance for many new artists to let their work be purchased since we live more and more in a digital world where even the aesthetics of avatars and in general of any digital good has a higher specific weight than in the past, so users are willing to pay more and more for aesthetics. As a matter of fact, Chainalysis tracked a minimum of 44.2 billion dollar worth of cryptocurrency sent to ERC-721 and ERC-1155 contracts, the two types of Ethereum smart contracts associated with NFT marketplaces and collections. The comparison with the previous year highlights a real consistent growth of the market since the value of 2020 was 106 million dollars. Someone says that it could be a speculative bubble, which indicates a situation in which the price is not justified. Very high margins and the promotion of the financial opportunity by influencers have attracted many users, so even big companies started to play a role on the network such as the NBA, which is one of the first companies to launch their exclusive collection. The prices of NFTs and in general some cryptocurrencies are so high for a reason: the trust that the market has in these assets. Investors really believe that these goods can be the future so they are willing to spend money on them. There are several steps to carry out for

creating an NFT, the first is to think about the art piece (with a very loose significate) we want to put on the market; then it is required the creation of a wallet since it is mandatory for any economic activity in a blockchain. Then is it possible to use DAPPS to sell your work, the most famous and important is Opensea, in which the access must be done with the wallet. It is possible to create your NFT collection directly on Opensea and in the collection you can just upload the "art" piece you selected. In Opensea it is possible to select many selling options: Set Price, Highest Bid, and Bundle. The platform takes 2.5% of the selling price as a fee, and also Gas fee must be considered when setting the price.

How blockchain technologies can be exploited by money launders

3.1 Money laundering Mechanism

There are many ways to launder money, from the simple to the very complex. One of the most common techniques is to use a legitimate, cash-based business owned by a criminal organization. For example, if the organization owns a restaurant, it might inflate the daily cash receipts to funnel illegal cash through the restaurant and into the restaurant's bank account. After that, the funds can be withdrawn as needed. These types of businesses are often referred to as "fronts." One common form of money laundering is called smurfing (also known as "structuring"). This is where the criminal breaks up large chunks of cash into multiple small deposits, often spreading them over many different accounts, to avoid detection. Money laundering can also be accomplished through the use of currency exchanges, wire transfers, and "mules"—cash smugglers, who sneak large amounts of cash across borders and deposit them in foreign accounts, where money-laundering enforcement is less strict.

Other money-laundering methods include:

- Investing in commodities such as gems and gold that can be moved easily to other jurisdictions;
- Discreetly investing in and selling valuable assets such as real estate, cars, and boats;
- Gambling and laundering money at casinos;
- Counterfeiting; and
- Using shell companies (inactive companies or corporations that essentially exist on paper only).

All these procedures can be easily exported in a blockchain environment, criminals exploit the anonymity provided by the system to launder gains from on-chain and off-chain crimes, they aim to obfuscate the source of money and at the same time convert the same money into cash for bank deposit. The most popular Virtual Assets Service Providers (VASPs) are subject to Financial Action Task Force (FATF) guidance, which aims to mitigate the risks of using virtual assets for money laundering and terrorist financing. FATF implements a risk-based approach to Anti-Money Laundering (AML) that includes Know Your Customer (KYC) regulations that require exchanges and other VASPs to verify their customers' identities. The Financial Action Task Force (on Money Laundering) (FATF) is an intergovernmental organization founded in 1989 on the initiative of the G7 to develop policies to combat money laundering. KYC is a set of

guidelines that prevent businesses from being used by criminal elements for money laundering; KYC has some key points that must be assessed :

- Customer acceptance policy;
- Customer identification procedures;
- Monitoring of transactions;
- Risk management.

In Italy “Banca d’Italia” sets the KYC requirements.

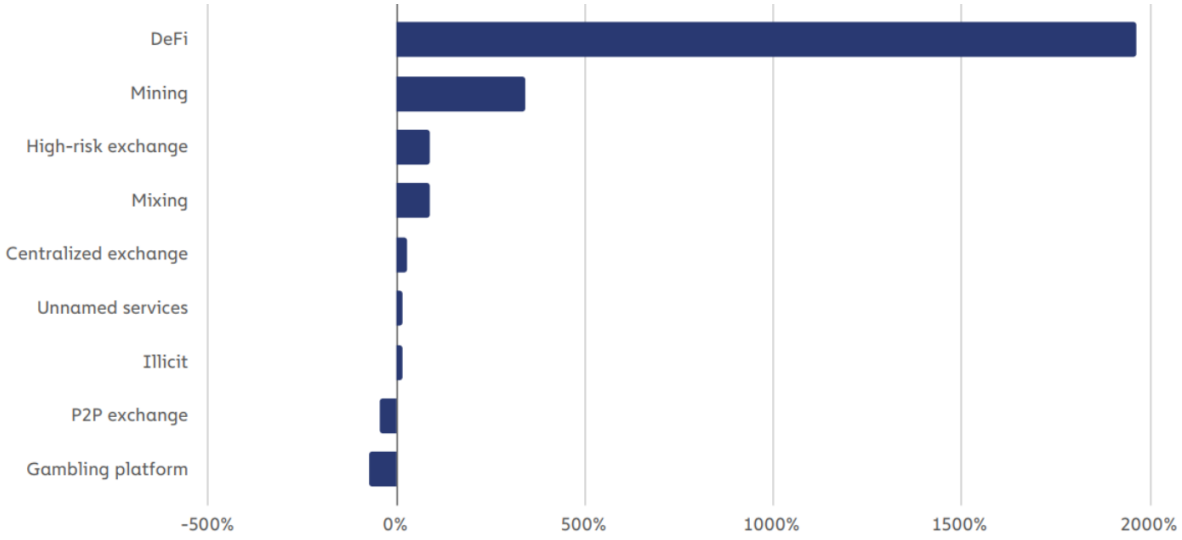
There are 5 principal methods to launder money in a blockchain

1. Nested services: are a broad category of services that operate within one or more exchanges. These services utilize addresses hosted by the exchanges to tap into the liquidity of the exchanges and capitalize on opportunities to trade. Some exchanges don’t require high compliance standards for nested services, allowing bad actors to exploit them for money laundering. On the blockchain ledger, these nested services transactions appear as having been conducted by their host counterparties (i.e., the exchanges) rather than by the hosted nested services or individuals’ addresses. The most famous nested service is called “OTC broker” (over-the-counter), it is so popular because guarantees ease of use and safety; OTC brokers allow direct communication between two parties without the mediation of an exchange, the broker does not take part in the negotiations, it only takes a commission. Once terms are defined, the parties transfer the custody of the assets through the broker. Transactions can happen between the same cryptocurrency or also different ones and even fiat currencies.
2. Gambling platforms: are also popular since it is possible to load money also via anonymous accounts; money are ore paced in a bet or directly paid out, when money are paid from the gambling platform gain legal status. This method for money laundering has been analysed by the (FATF) in a report published in 2020 in which gambling services can be considered a red flag for investigators.
3. Mixers: are services that tie together many assets coming from many different addresses and then release them at random intervals to new destinations, e.g. wallets; they are often used to conceal the trail of funds before they are transferred to legitimate businesses or major exchanges. This increases a lot of anonymity and traceability. A case reported by the United States Department of Justice involves the mixer Helix, the indictment alleges that Helix moved over 350,000 bitcoin, valued at over $300 million at the time of the transactions. The man who operated this system was charged with money

laundering conspiracy, operating an unlicensed money transmitting business, and conducting money transmission without a D.C. license.

4. DeFi: “decentralized finance” refers to a class of decentralized cryptocurrency platforms that can run autonomously without the support of a central company, group, or person. They are based on a set of smart contracts and can fulfill specific financial functions determined by them; decentralized exchanges and lending platforms. DeFi protocols saw the most growth by far in usage for money laundering at 1 964%
5. Services headquartered in high-risk jurisdictions: are services that refer to jurisdictions where there is not an enough strong AML policy.

Since 2017 cybercriminals have laundered about 33 million dollars, 8.6 only in 2021 a 30% increase by 2020; these stats take into account only money derived by cybercriminal activities, it is much harder to assess how much money derived by fiat currencies for offline crimes. The methods for laundering are rapidly changing as this graph, in the Chainanalysis crypto crime report, states:



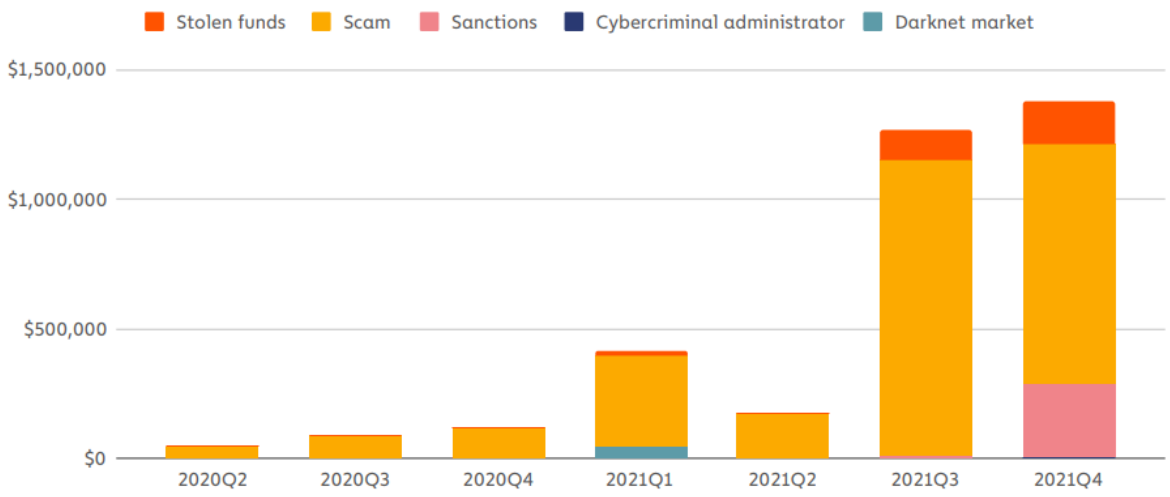
This plot shows the percentage growth of these services in a year so from 2020 to 2021. Here it is clear how Defi platforms are taking the scene even if there is a huge increase in the mining activity and in mixers. Gambling and p2p exchanges become less popular because of their efficiency and traceability.

Since the scarcity of these services ML activity is very concentrated, but from 2020 to 2021 the trend is decreasing in 2020 55% of all cryptocurrency sent from illicit addresses went to just 270 service deposit addresses. In 2021 a group of just 583 deposit addresses received 54% of all funds sent from illicit addresses

in 2021. Each of those 583 addresses received at least $1 million from illicit addresses, and in total, they received just under $2.5 billion worth of cryptocurrency. An even smaller group of 45 addresses received 24% of all funds sent from illicit addresses for a total of just under $1.1 billion. One deposit address received just over $200 million, all from wallets associated with the Finiko Ponzi scheme. This shifting is due to the increased efforts by the institution to prevent ML, so criminals are starting to use other channels to get even more harder to trace.

NFTs are attractive for money launders because they are fully digital, making them much easier to trade compared to moving physical art. Like with cryptocurrencies, an NFT can be transferred from one wallet or owner to another within seconds. There are other reasons but are more technical, the first is the very high price volatility: while the exchange rate of the main crypto to the most important fiat currencies follows the market principles of supply and demand, the prices of NFTs are highly speculative. The second reason is the total anonymity provided by the system. Another point that makes NFTs ML appetible to criminals is the legal framework. I wrote in the 1.5 paragraph 6AMLD is the rule that covers the ML in the art sector but this directive does not specify NFT as an art form so KYC and CDD are not applicable.

The reality is that money laundering through NFTs is a phenomenon that, although it is growing, plays a not very important role in laundering through cryptocurrencies. The value sent to NFT marketplaces by illicit addresses jumped significantly in 2021, as this plot from Chainanalysis states.



The impact of NFTs money laundering on the 8.6 billion cryptocurrency-based money laundering is very low for now but it must not be undervalued because of a large risk to building trust in NFTs.

3.2 AML Mechanism

In 2014 The Financial Action Task Force (FATF) establishes global standards for anti-money laundering legislation. In 2014 the FATF published cryptocurrency AML guidance, in which is recommended to apply KYC process also in the blockchain environment. It is divided into three different steps :

1. Customer Identification (CIP): customer identification program, or 'CIP,' verifies that the customer is who they claim to be by utilizing reliable and independent data. Verification information may include: the client's legal name, date of birth, address, and verifying documentation such as a driver's license or passport. business licenses and articles of incorporation are frequently required of enterprise customers.
2. Customer Due Diligence (CDD): I have already treated this argument however financial service providers must assess the risk rating of the individual based on background checks, customer surveys, and reviews of the client transaction history.
3. Continuous monitoring: that is constantly reviewing transactions for signs of criminal activity. When suspicious activity is discovered, VASPs are required to file Suspicious Activity Reports (SARs) with FinCEN or other appropriate law enforcement agencies.

These procedures are performed by the virtual asset service providers (VASPs) that the FATF defined to include crypto exchanges, stablecoin issuers, and, on a case-by-case basis, some DeFi protocols and NFT marketplaces. When suspicious activity is observed, VASPs report this information to relevant regulators and agencies, which then use blockchain analysis tools to investigate the flow of funds and link illicit activity to real-world identifiers.

The biggest difference between fiat and cryptocurrency-based money laundering is that,

due to the inherent transparency of blockchains, the movements of cryptocurrency can be retrieved between wallets and services in their efforts to convert their funds

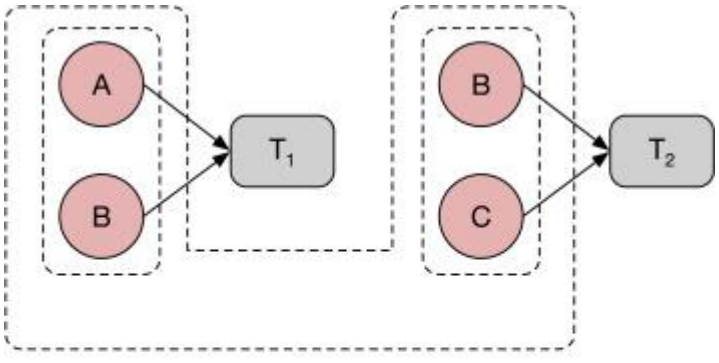
into cash. It is impossible to track all money laundering activity by measuring the value sent from known criminal addresses. As stated above, some criminals use

cryptocurrency to launder funds from crimes that happen offline, and there are many

criminal addresses in use that have yet to be identified. However, investigators can account for some of these more obscured instances of money laundering by looking for transaction patterns suggesting that users were trying to avoid compliance screens. For instance, due to regulations like the Travel Rule, cryptocurrency businesses in many countries must conduct additional compliance checks, reporting, and information sharing related to transactions above $1,000 USD in value. As you might expect, illicit addresses send a disproportionate number of transfers to exchanges just below that $1,000 threshold. Law enforcement must become proficient in analyzing DeFi transactions in order to crack cases like that of the Spartan Protocol hack, but the teams behind DeFi protocols must also work to prevent their products from being abused by cybercriminals. One way they can do that is by screening the wallets interacting with their smart contracts for prior transactions with known illicit addresses.

The typical beginning of an investigation is to track the movements of a suspicious address, then it must be de-anonymized. Blockchain analysis assesses this problem by combining two methods: *Address clustering heuristics* and *Attribution tags.*

The first is considered one of the most effective clustering heuristics, suppose two addresses are input of a transaction, then if one of the two is used as an input for another transaction along with a new address it is very likely that the three addresses are controlled by the same person that has made both the transactions.



a **Multi-Input Clustering Heuristics**: Addresses *A* and *B* are inputs of transaction T_1 and must therefore be controlled by the owner of the corresponding private keys. The same holds for addresses *B* and *C* of T_2. Since address *B* occurs in the set of inputs of T_1 and T_2 one can infer that addresses *A*, *B*, *C*, and *D* are controlled by the same actor.

There are ways to circumvent this detection method, the most famous is called *CoinJoin*: in this protocol *n* parties produce a special joint transaction so the relationships between inputs and outputs are hided and, in the end, who of the n parties transacted with whom. that is interpreted by the clustering as a unique group ignoring that are independent part involved in a single cluster. Some studies have assessed the accuracy of this technique, showing that on average 69.34% of the addresses could be linked; the research was made on a dataset consisting of 37 585 user wallets.

Attribution tags give contextual information on a cryptocurrency address, transaction, or cluster. It does not rely on static, predefined taxonomic structures but on dynamic, community-driven linguistic terms and conceptions.

The combination of these two methods is able to discover many relationships and personally identifiable information.

3.3 Money laundering vs wash trading

Wash trading is a phenomenon aimed to increase the market value of an asset. An investor sells and buys himself the same asset many times. The reason this practice is illegal is because it creates misleading and artificial activities in the market: the object seems more requested than how actually is, and it generates commission fees to brokers in order to compensate them for something that cannot be openly paid for.

In the case of NFTs it is very easy to make this infringement since many NFT trading platforms allow users to trade by simply connecting their wallet to the platform, with no need to identify themselves.

Thanks to blockchain analysis it is possible to detect this activity simply by tracking sales of NFTs. If the buyer has received tokens by the account of the seller in some way wash trading is detected. Analysis of NFT sales to self-financed addresses shows that some NFT sellers have conducted hundreds of wash trades.

How criminal activities can be detected

4.1 Blockchain analysis platforms and Maltego

For Blockchain analysis platforms I mean all the services aimed to investigate all the activities performed in a blockchain. It is very common that the companies that run these platforms to publish reports about some specific activities or trends in a blockchain. One of the most efficient and famous is Maltego which I used to do my own investigation. It is fair to say that Maltego is not a specific tool it can be used to perform any investigation regarding the cyber field. His strongness stands in the deployment of graphs which allow the investigator to trace each movement and to spot hidden links between elements. Working with this software is not trivial, there is the need for the user to follow some courses in order to fully understand the functionalities and capabilities of the tool. Depending on the investigation Maltego offers different "Plug-ins" in order to better fit the needs of the user, these features are not always developed by Maltego though. They are called *transforms*, a set of functions that must be applied to the correct *entity*, which is the node of the graph and stands for a specific object. Thanks to transforms is it possible to retrieve specific information, such as the location or IP address of an entity, but they are able to retrieve other entities starting by one, to see how the first entity is linked in the environment.

For my specific tasks there is a specific transform to use it is called CypherTrace, it allows to: trace blockchain transactions, retrieve the wallet by an address, retrieve the country from a wallet, trace inbound and outbound transactions for an address, and to assess the risk score of transactions and accounts. CypherTrace is not included in any Maltego version is not included in any version of; Maltego not even in mine, a pro version I got to carry out the study of this paper.

So even if I tried to reach out CypherTrace support I could not be able to get a license since they offer their service to businesses. Even if the right way to conduct the investigation is not feasible by a student I decided to perform my analysis using another transform in Maltego called Tatum Blockchain Explorer. This tool is able to identify the parties of a transaction and to trace inbound and outbound transactions for an address.

There are also online tools that can be used for an investigation purposes such as *Etherscan*, which I used for my study as well. Etherscan.io is an independent Ethereum-based block explorer. The Etherscan app keeps track of blockchain transactions on the Ethereum network. It is useful for this paper goal because keeps a record of any NFT in the Blockchain and for each of them stores all the changes of ownership.

4.2 Practical implementation in the Maltego platform

In this section will be discussed how an investigation can be carried out using Maltego.

The main idea is to analyze NFT transactions in order to find *suspect behaviors* and then consider the accounts involved and draw some conclusions. Suspect behaviors are defined by FATF in a specific paper called “Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing”.

There are many indicators to detect Money laundering, one of them is the type of transaction involved. The next points illustrate which types of transactions have a high risk of Money laundering.

- Many payments in small amounts to avoid attracting attention.
- High-value cryptocurrency transactions in only a short period.
- Instantly transferring virtual funds out of highly controlled areas and into low-regulated dominions.
- Immediately withdrawing virtual funds without any in-between transactions.
- Depositing previously identified stolen funds into crypto wallets.

There are also some patterns that identify this activity, such as :

- New accounts that are seemingly inconsistent with the opener’s determined wealth.
- New accounts funded by a hefty preliminary payment that is shortly afterward traded.
- Transactions with seemingly illogical sets of cryptocurrencies or accounts without ties.
- Large amounts of cryptocurrencies exchanged recurrently within a period to one account from numerous others.
- Small quantities from multiple virtual wallets that are instantly relocated or removed.
- A series of crypto movements resulting in a loss of money due to account fees.
- Recurrent exchanges of fiat money to cryptocurrency without apparent reason.

Also the identity of the parties must be considered for detecting ML, an account with poor information or not compliant with KYC is a possible suspect. In particular, if the account has a suspicious IP address or it is registered in a high-risk jurisdiction. The profile is considered suspicious even if :

- Accounts with shared identification credentials or illegal activity associated with them
- Accounts showing dissimilarity between the IP address on account and the IP address of the transactions
- Customers repeatedly adjus their identification information or contact forms
- Customers attempting to access the platform from multiple IP addresses within a single day or short period
- Accounts showing significant gains or losses by performing trades with the same individuals
- Accounts communicating with each other in a way that indicates illicit activities
- Transactions using more than one cryptocurrency type, especially highly anonymous currencies with seemingly “unjustified” high feeds
- Movement of funds from a transparent blockchain account to a centralized cryptocurrency exchange platform and then to a private or anonymous coin or currency
- Customers operating as unlicensed providers for other users on peer-to-peer cryptocurrency sites who may frequently charge high fees to handle the virtual funds on behalf of their patrons than a licensed company
- A substantial volume of peer-to-peer transaction activity using mixing services without justification
- Funds from a suspicious source deposited into a cryptocurrency wallet, such as gambling sites
- Funds entering cryptocurrency wallets from suspicious IP addresses or managed with encryption software
- Funds transferred across international borders using decentralized hardware
- Users who use proxies or DNS allow users to hide domain names while registering for a cryptocurrency wallet
- Multiple virtual wallets, all from a singular IP address
- Usage of undocumented cryptocurrencies linked to fraud

- Funds sent with clearly insufficient customer due diligence (CDD) or know-your-customer (KYC) procedures
- The use of virtual currency ATMs for numerous minor transactions in high-risk jurisdictions

There are also other red flags Involving the source of the money and Money Mules but with the instrument used in this paper is impossible to take into consideration also these aspects.

To start the investigation I downloaded from Etherscan three distinct csv files (unfortunately Etherscan allows only to download 1000 records) and merged them into a single file (see Appendix [1]). It contains NFT transaction information from 07/09/2022 to 08/09/2022. But it is a good starting point.

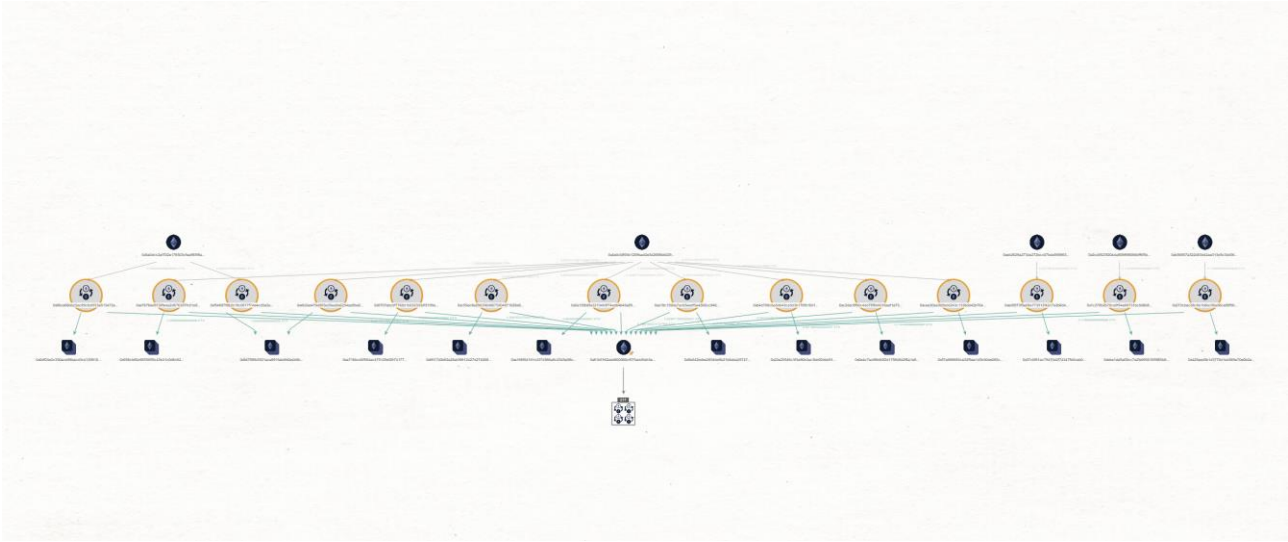
The file contains 11 columns and 3000 rows. The attributes are :

- Transaction hash
- UnixTimestamp
- Date Time (UTC)
- Action
- Buyer
- NFT
- Token ID
- Type
- Quantity
- Price
- Market.

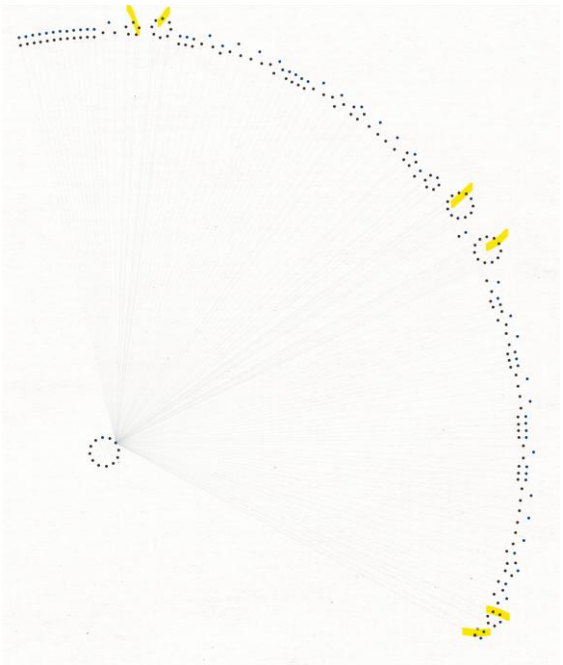
The variables' names are quite self-explaining, the only thing that must be highlighted is that a single NFT can be identified by combining two keys: "NFT" and "Token ID". Once data have been collected, it is useful to explore them in order to retrieve relevant information. To do that I used a software called RapidMiner, which is very fast and useful for exploratory data analysis. I started removing duplicates and the records shifted from 3000 to about 2000, then I decided to look for 2 distinct possible investigative leads. The first is to identify the most traded NFT on that day and the second was to identify the most active buyers during the same period.

The buyer who appears the most in the csv file has this address and seems to have 0 transactions made in his history, I double-checked the id by using Maltego and Etherscan, thus we can clearly spot the first red flag.

The second one in the list has instead a recorded activity, a few incoming transactions, and 217 outgoing ones. Analysing inbound transactions we can figure out to which block each transaction belongs and who is the sender. As we can see from the graph we can spot that the majority of the inbound transactions belong to a single address, this can be interesting since FATF specifies that ML is carried out by many small transactions.



Now the focus shifts toward the outbound transaction. Once applied the transform that identifies the receiver, the graph becomes messy and I decide to change the visualization for a better understanding. The situation is clear many transactions are deployed to the same accounts, now the graph looks like this.



The crossed areas are the ones that worry more since a considerable number of transactions are directed to the same user. At this point is worth checking the suspicious addresses.

The first (0x00000000006c3852cbEf3e08E8dF289169EdE581) refers to a new web3 market protocol called Seaport 1.1 this could lead to further investigations since the unknown nature of this exchange it is impossible to draw any consistent conclusion.

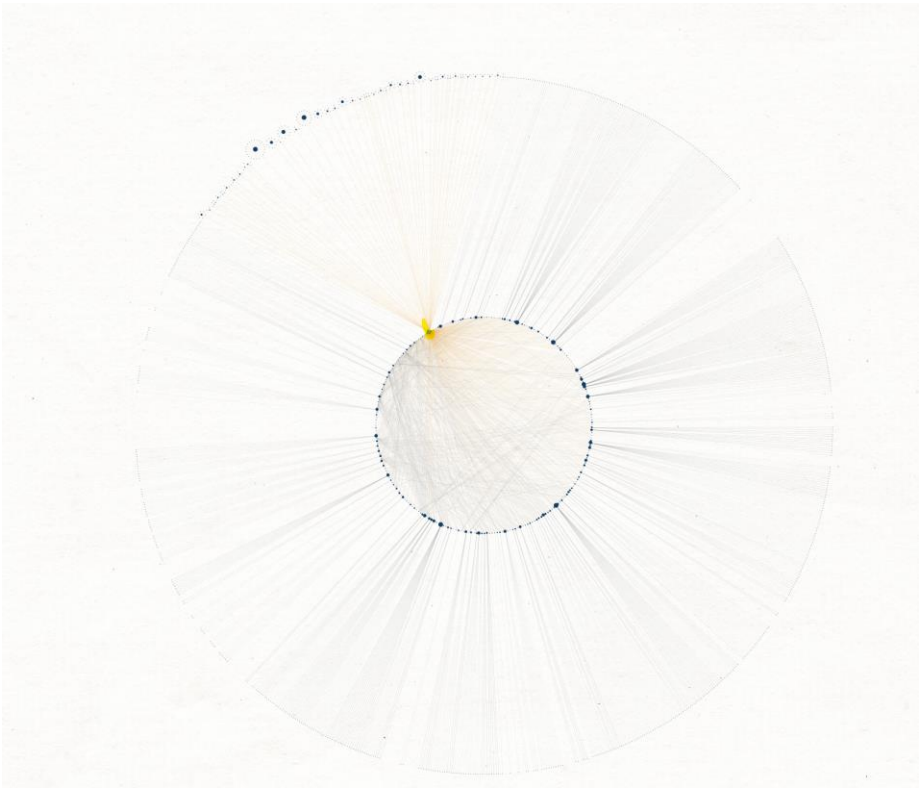
The second (0x7f268357A8c2552623316e2562D90e642bB538E5) is linked to another protocol called Wyvern exchange, which still could be considered suspicious even if this protocol will be implemented in Opensea. The third (0x7CB90567a118cd9F6CA326067A0813b289bdCb54) is linked to a NFT collection called Apes Together Strong. The remaining address(0xC58fC4693b3170dE0c1DcD2C0b0aF8EECfB3186f, 0xBd88151ca39e06A94063248972cEE5030D0af46f, 0x98B4182F14b49aAC87E3d64B6AE69d3aaB1dc913) seem to be linked with other NFTs collections (See appendix [2] for the graph).

Now can take place the second investigation method (see appendix [3],[4],[5]) that starts from an NFT transaction. First of all, it is important to figure out which NFTs are traded the most during that period. Rapid Miner is not able to process some token id since they can be composed by 75 or more digits, so the program assigns to each id over maxint the same value, and thus it collects all the token IDs all together. To avoid this misleading error I checked personally on the CSV file each token id. Since the first three positions in the list obtained by the workflow suffer from this problem, the most traded NFT is the fourth: RTFKT Clone X Forging SZN 1 with the id of 74.

The next step is to check the CSV file to retrieve a transaction in which this token is involved. I used to start the investigation the transaction with this hash 0xcf5e6c2af8c1e06246bc6a6554aa5aef879c54fe9bc66ea800c7c37a5324a989.

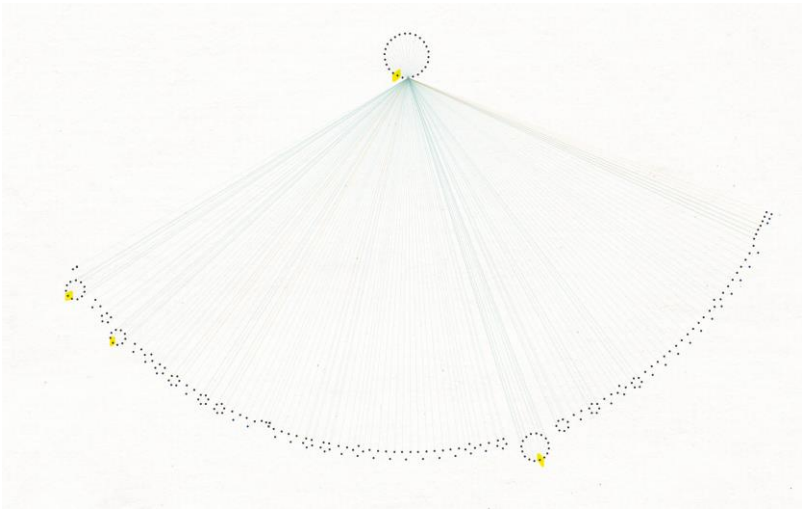
Once the parties of the transactions are retrieved, it is possible to follow the same process of the previous investigation to spot red flag behaviors.

The receiver has an address that it is already been discussed since it is Seaport1.1.



It is important to highlight that the Seport 1.1 node (in yellow) it is linked to all the major nodes that can be considered as *proxy nodes* which task is to gather transactions and root them to the *sink* node. Further analysis on proxy nodes could lead to discover some illegal activity.

The sender account (0x2b7e23c5f79ca72df79294728347abb2461aed91) presents very few in going transactions and a lot of outgoing ones.



Like the previous graphs, the yellow marked accounts are the ones that require some other investigation. The 3 of the spotted accounts belong to: Seaport 1.1, Wyvern exchange, and Synthetix which is a protocol providing the backbone for derivatives trading in DeFi. The last one (0xDef1C0ded9bec7F1a1670819833240f027b25EfF) leads us to a proxy node that must be considered for a deeper investigation in order to determine its nature.

Conclusions

Money laundering is one of the most recurrent illicit activities that exploit blockchains, it is crucial to monitor this phenomenon since there are billions of dollars are laundered every year. It is important to fight it because criminal groups such as terrorists or criminal hackers finance themselves through ML.

To sum up: NFTs money laundering does not affect the crypto-economy very much, although it is an increasing phenomenon; and it is for this reason that the thesis is also aimed at the development of an investigative method.

The Investigation method proposed in this paper can be applied in each scenario, since only basic information are necessary to start the investigation and this information are really easy to retrieve because they are public. The backtracking logic in my opinion can lead to very accurate results especially considering all the money laundering red flags discussed in the previous section.

Of course, this study could be more detailed and conclusive using more advanced instruments (e.g. CypherTrace), nevertheless, the obtained results are to be considered meaningful already at this stage.

With the methodology exposed earlier, the investigator is able to focus only on a few nodes and not all of the graph, as shown in the second investigation for example, in which from the Seaport graph derives that it is enough to analyze about a dozen of proxy nodes instead of over 300, so there is a remarkable reduction of investigation costs.

It is clear that to further investigate on suspicious nodes other facilities are required such as advanced software, a well-trained team and, of course, time.

Appendix

To download all the material please access to this link, you will find a copy of this work with all the working files.

[1]

CSV_finalwork.csv

[2]

First_suspect_links.mtgl

[3]

Transaction_inv.mtgl

[4]

Reciver.mtgl

[5]

Reciver.mtgl

[6]

Thesis_process.rmp

References

- https://www.1337pwn.com/how-to-extract-cryptocurrency-addresses-indicators-of-compromise-from-binaries-using-ransomcoin-tool/
- https://www.maltego.com/blog/bitcoin-forensics-with-maltego-and-ciphertrace-blockchain-intelligence/
- https://www.computerweekly.com/tip/Maltego-tutorial-Part-1-Information-gathering
- https://resources.infosecinstitute.com/topic/information-gathering-maltego/
- https://en.wikipedia.org/wiki/Money_laundering
- https://www.fatf-gafi.org/faq/moneylaundering/
- https://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-how-much-is-out-there.html
- https://www.napier.ai/post/financial-crime-statistics-2022#:~:text=The%20most%20common%20estimate%20for,or%20given%20as%20a%20range.
- https://www.unodc.org/unodc/en/money-laundering/overview.html
- https://www.consilium.europa.eu/it/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/
- https://weblog.metisoft.it/vi-direttiva-antiriciclaggio-6-novit%C3%A0-da-fine-2020#:~:text=La%20VI%20Direttiva%20Antiriciclaggio%20aumenta,in%20una%20Direttiva%20UE%20sul
- https://www.artandobject.com/news/how-money-laundering-works-art-world
- https://complyadvantage.com/insights/art-money-laundering/
- https://www.nytimes.com/2021/06/19/arts/design/money-laundering-art-market.html
- https://www.natlawreview.com/article/art-and-money-laundering
- https://complyadvantage.com/insights/aml-regulations-in-antiquities/
- https://www.theglobeandmail.com/report-on-business/international-business/european-business/economists-urge-tighter-regulations-to-curb-money-laundering-in-art-market/article26217852/
- https://itsartlaw.org/2022/07/26/lifting-the-veil-what-are-the-aml-due-diligence-requirements-for-the-art-market-in-the-united-states/

- https://it.wikipedia.org/wiki/Blockchain
- https://en.wikipedia.org/wiki/Ethereum
- https://decrypt.co/resources/what-is-ethereum-2-0
- https://ethereum.org/it/developers/docs/consensus-mechanisms/pos/
- https://en.wikipedia.org/wiki/Non-fungible_token
- https://www.artsy.net/article/artsy-editorial-8-artists-making-nfts
- https://en.wikipedia.org/wiki/Web3
- https://101blockchains.com/disadvantages-of-blockchain/
- https://www.investopedia.com/terms/m/moneylaundering.asp#:~:text=The%20process%20of%20laundering%20money,of%20transactions%20and%20bookkeeping%20tricks.
- https://www.bbc.com/news/technology-60072195
- https://www.forbes.com/sites/forbesbusinesscouncil/2021/06/23/trends-in-blockchain-why-big-banks-are-adopting-this-technology/?sh=13b6fb3551e2
- https://www.cognyte.com/blog/anti-money-laundering-cryptocurrency/
- https://en.wikipedia.org/wiki/Financial_Action_Task_Force
- https://en.wikipedia.org/wiki/Know_your_customer#:~:text=The%20know%20your%20customer%20or,money%20laundering%20(AML)%20policy.
- https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf
- https://www.justice.gov/opa/pr/ohio-resident-charged-operating-darknet-based-bitcoin-mixer-which-laundered-over-300-million
- https://www.frontiersin.org/articles/10.3389/fphy.2021.665399/full
- https://www.makeuseof.com/how-nfts-used-wash-trading-money-laundering/
- https://complyadvantage.com/insights/nft-money-laundering-what-you-need-to-know/
- https://www.fatf-gafi.org/media/fatf/documents/recommendations/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf
- https://notabene.id/crypto-travel-rule-101/aml-crypto
- https://blog.chainalysis.com/reports/what-is-aml-and-kyc-for-crypto/
- https://baselgovernance.org/sites/default/files/2021-08/QG%20crypto%20money%20laundering%20updated.pdf
- https://www.imolin.org/pdf/UNODC_VirtualCurrencies_final_EN_Print.pdf
- https://www.sciencedirect.com/science/article/pii/S1742287619302567#:~:text=Introduction,forensic%20method%20in%20law%20enforcement.

- https://arxiv.org/pdf/1908.02591.pdf
- https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-nft-wash-trading-money-laundering/
- https://www.google.com/search?q=Neo4j&oq=Neo4j&aqs=chrome..69i57j0i512l9.1652j0j15&sourceid=chrome&ie=UTF-8
- https://financialcrimeacademy.org/cryptocurrency-money-laundering-red-flags/

- https://www.imf.org/en/Publications/fandd/issues/2019/09/the-art-of-money-laundering-and-washing-illicit-cash-mashberg#:~:text=According%20to%20the%20United%20Nations,much%20as%20%246%20billion%20annually.
- 
Bitcoin_Crypto_Coins_ and_Global_Anti_Mo.p
- 
Chainalysis NFT Market Report.pdf
- 
Chainalysis-Crypto-Crime-2021.pdf
- 
Crypto-Crime-Report-2022.pdf
- 
LEGAL_REMARKS_ON_THE_OVERARCHING_
-

Virtual-Assets-Red-Flag-Indicators.pdf