The comparative analysis of regulations in the Italian Republic and the Russian Federation against cryptolaundering techniques

The comparative analysis of crypto laundering techniques in the Italian Republic and the Russian Federation

Katsiaryna Bahamazava

Department of Economics and Statistics "Cognetti de Martiis", University of Turin, Turin, Italy,

and

Stanley Reznik

Department of Special Projects, Trinity Resources LLC., German Town, MD, USA

Abstract

Purpose – In the age of DarkNetMarkets proliferation, combatting money laundering has become even more complicated. Constantly evolving technologies add a new layer of difficulty to already intricated schemes of hiding the cryptocurrency's origin. Considering the latest development of cryptocurrency- and blockchain-related use cases, this study aims to scrutinize Italian and Russian anti money laundering regulations to understand their preparedness for a new era of laundering possibilities.

Design/methodology/approach – One of the most recommended ways to buy and sell cryptocurrencies for illegal drug trade on DarkNet was discovered using machine learning, i.e. natural language processing and topic modeling. This study compares how current Italian and Russian laws address this technique.

Findings – Despite differences in cryptocurrency regulation, both the Italian Republic and the Russian Federation fall behind on preventing crypto laundering.

Originality/value – The main contributions of this paper: consideration of noncustodial wallet projects and nonfungible token platforms through the lens of money laundering opportunities, comparison of Italian and Russian anti money laundering regulations related to cryptocurrency, empirical analysis of the preferred method of trading/exchanging cryptocurrency for DarkNet illegal trade using machine learning techniques and the assessment of how Italian and Russian regulations address these money laundering methods.

Keywords: Money laundering, Cryptocurrency, DarkNetMarkets, Drugs, Machine learning
Paper type: Research paper

1. Introduction

Advances in modern technologies introduce new opportunities for businesses and people while providing challenges for regulators. One of the main challenges is the use of digital innovations to commit crimes. Money laundering being a crime by itself is often used

to trace another illegal activity, otherwise, undiscovered. Therefore, it is possible to use crypto laundering schemes to investigate other crimes like the illegal drug trade on DarkNet, which otherwise is difficult to scrutinize. However, the borderless nature of cryptocurrencies and all blockchain-based technologies bring another layer of complexity for regulators. Notwithstanding the progress made in cryptocurrency regulations, criminals are one step ahead in utilizing newer technologies.

The Italian Republic and the Russian Federation both follow the same international guidelines in their fight against crypto laundering. Italian laws are based on custodianship, and all custodial platforms must comply with AML/CFT regulations. Russian laws govern all crypto-related activity regardless of custodianship solely based on whether platforms are using Russian infrastructure and/or locations. We will show in a case study the use of non-custodial wallet in view of anti-money laundering regulations of the Italian Republic and Russian Federation.

Consider Internet consisting of layers, "surface[1]" layer or ClearNet, and "deep[2]" layer (Deep Web). The DarkWeb[3] (DarkNet) is the deepest layer of the Deep Web. There are few different ways to reach the DarkNet, and the most common way is through The Onion Router[4] (TOR). People use TOR as a browser to anonymously reach the DarkNet. In August 2020, TOR had at least 2,171,353 daily accesses worldwide [TOR, 2020]. DarkNet hosts web sites known as DarkNetMarkets (DNMs). DNMs operate like usual e-commerce businesses such as eBay and Amazon, with enhanced anonymity. DNMs are widely popular platforms, and users spent approximately 1 billion USD in 2018 on these markets [Europol, 2019].

Based on DNMs' perceived anonymity, protection, and convenience, customers choose to buy illegal goods and services there [UN, 2020]. All DNM users are interested in concealing the origin of their cryptocurrency. Transactions done in crypto are written in the corresponding blockchain, which means that it is possible to trace the origin of the payment using specific techniques. Buyers are interested in obscuring their connection with cryptocurrency intended for DNM trades, sellers need to "clean" profit obtained from illegal activity on DNMs, and platform owners seek to conceal the origin of fees they earned from DNM vendors.

Money laundering is defined by UN Vienna 1988 Convention (article 3.1):

"the conversion or transfer of property, knowing that such property is derived from any offence(s), for the purpose of concealing or disguising the illicit origin of the property or

[1] "Surface" Web - everyday part of the Internet accessible by search engines as Google [Weimann, G., 2016.].

[2] "Deep" Web is everything not discoverable with search engines, including password-protected sites and encrypted networks [Shillito, M.R., 2019].

[3] Dark Web is a portion of the Deep Web that contains intentionally concealed content [Shillito, M.R., 2019].

[4] TOR is a free network designed to anonymise your real Internet Protocol address by routing your traffic through many servers of the TOR network [Europol, 2014].

of assisting any person who is involved in such offence(s) to evade the legal consequences of his actions" [UNODC, 2021]. Member countries, among which are Italian Republic and Russian Federation, adopted measures to criminalize money laundering offenses.

One of the measures to combat international money laundering is membership in FATF. "The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions[7]" [FATF, 2021]. FATF was organized to set standards and advance the effective application of "legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation, and other related threats to the integrity of the international financial system" [ibid].

Due to the proliferation of new technologies, innovative methods to conceal the origin of cryptocurrencies have appeared. These methods consist of the use of crypto-exchanges, non-custodial wallet-mixers, Decentralized Finance (DeFi) projects, and Non-Fungible Token (NFT) platforms.

Crypto exchanges are entities or persons who offer exchange services for cryptocurrency users, usually for a fee [Houben and Snyers, 2018].

Wallet-mixer (tumbler) is a service that enables customers, for a fee, to send cryptocurrency to designated recipients in a manner that was designed to conceal and obfuscate the original owner (or the source) of the cryptocurrency [US Department of Justice, 2020].

Decentralized Finance project (DeFi) is a common term that incorporates decentralization, blockchain, smart contracts[5], disintermediation, open banking [Zetzsche, Arner and Buckley, 2020].
Non-Fungible token (NFT) "represents a one-of-a-kind digital asset which has been securitised by the backing of cryptography and thus allows the owner to claim their creation" [NFTically, 2021]. In other terms, NFT is proof of ownership of any digital artwork.

The paper's main objective is to consider new opportunities for money laundering which offer cryptocurrency-related projects and the challenges for regulators to combat them.

Due to the novelty of such phenomena as cryptocurrency (the first successful cryptocurrency, Bitcoin, was created in 2008), DNMs (first DNM "Silk Road" was created in 2011), DeFi (2018 [Coinmarketcap, 2021]), and NFT (2014 [The New York Times Magazine, 2021]) the paper hypothesizes that anti-money laundering regulations are not fully equipped to cover crypto laundering schemes. To check the hypothesis, the following research questions (RQ) were asked:

[5] "Smart-contract is an algorithm that is characterized by the presence of the following elements: 1) there is an agreement that defines a set of promises that are declined in a set of clauses; 2) the agreement is written in digital form, through a program or software that incorporates these clauses; and 3) the agreement is formalized by a protocol that established how the parties must process the qualitative and quantitative information of the contract, thereby allowing the parties to satisfy the contractual terms" [Carlo Gola and Andrea Caponera, 2019]. For more on smart-contract's regulatory issues, see [Grundmann and Hacker, 2017].

1. How do Italian and Russian regulators address the crypto laundering threat? What are the aforementioned crypto laundering techniques?
2. What are the differences in those regulations?
3. What was the most recommended crypto laundering method by DarkNet forum users, and how does it relate to the laws of the Italian Republic and Russian Federation?

To answer the first research question, the functional method [Van Hoecke, 2011] of comparative legal research was used. This method was chosen since it concentrates on similarities/differences of rules' results (social or legal) rather than the pure legal approach. Furthermore, the existing laws related to crypto laundering were examined with the evaluative research type.

For the second research question, the laws related to crypto laundering were examined from an economic point of view.

To answer the third research question, we utilized the unsupervised machine learning approach. We applied Natural Language Processing (NLP) techniques and topic models to reveal the most popular method for exchanging and manipulating cryptocurrency. Then, we consider the revealed method through the prism of anti-money laundering laws and regulations in the Italian Republic and the Russian Federation.

The main contributions of this paper:

a. Consideration of non-custodial wallet projects and NFT platforms through the lens of money laundering opportunities,
b. Comparison of Italian and Russian anti-money laundering regulations related to cryptocurrency
c. Empirical analysis of the preferred method of trading/exchanging cryptocurrency for DarkNet illegal trade using machine learning techniques.
d. The assessment of how Italian and Russian regulations address these money laundering methods.

The paper has following sections. Section 2 is the literature review. Section 3 provides the stylized facts of the aforementioned crypto laundering techniques. In the Section 4, the analysis of Financial Action Task Force (FATF) recommendations against crypto laundering techniques is presented. Section 5 examines specific laws confronting laundering cryptocurrency in Italian Republic. Then, Section 6 reviews the legislation in Russian Federation addressing crypto laundering. Next, in Section 7 we provide comparative analysis of Russian and Italian regulations against laundering techniques. Section 8 demonstrates the case study with the unsupervised machine learning inquiry results on the preferred method of DarkWeb users to exchange cryptocurrency. Section 9 concludes.

2. Literature review

B. Walker-Munro analyzed the problem of criminal law regulators in adapting to technological change [Walker-Munro, B., 2020]. The author considered how new technologies (DarkWeb) exacerbated the old problem (the supply of illicit drugs). Furthermore, he showed

how cyber-systemics could be attractive for criminal law regulators in times of technological disruption.

I. Adeleke et al. applied the Systematic Quantitative Assessment Technique to analyze the cryptocurrency scholarship [I. Adeleke et al., 2019]. The authors found that most papers focused on problems of cryptocurrency regulation without providing any recommendations.

D. Bryans compared Bitcoin to other currency systems and showed the potential for money laundering using bitcoin blockchain [Bryans, 2014]. Unfortunately, Bitcoin is thought to be untraceable at the time of writing, which is not true.

V. Dyntu and O.Dykyi analyzed the challenges and opportunities that the Fourth Industrial Revolution brought to law regulators through such a new phenomenon as the digital economy [V. Dyntu and O.Dykyi, 2018]. The authors examined how Bitcoin could facilitate money laundering.

T.A. Frick reviewed the international development in lieu of money laundering through cryptocurrency [T.A. Frick, 2019]. Furthermore, he compared the E.U. developments with the Swiss approach. Out of the author's analysis, the Swiss approach to anti-money laundering in the case of cryptocurrency usage was more effective.

M. Campbell-Verduyn argued that Bitcoin and other cryptocurrencies posed a more theoretical threat to be used in money laundering schemes than actual [M. Campbell-Verduyn, 2018]. Furthermore, the author considered the possibilities that cryptocurrency could give to combat money laundering globally.

V.A.Kinsburskaya compared the FATF recommendations and Russian regulation related to cryptocurrency usage [V.A.Kinsburskaya, 2019]. The author analyzed criminal cases (mostly related to illegal drug trade) where cryptocurrencies were utilized and proposed strengthening control over the transactions where cryptocurrency is exchanged for fiat money.

L. Haffke et al. considered the shortcomings of the 5th AML EU Directive [L. Haffke et al., 2020]. The authors gave an overview of possible cryptocurrency-related services and presented the hypothetical money laundering scenario with cryptocurrency. They showed that the 5th AML EU Directive created an ambiguity with the "virtual currencies" definition covering only currency tokens. From this uncertainty follows that only cryptocurrency exchanges trading currency tokens are regulated. Moreover, providers engaged in trading solely cryptocurrency are not covered by the 5th AML EU Directive. However, if these providers "safeguard private cryptographic keys on behalf of its customers," they are regulated by the Directive. Wallet providers who do not store their customers' private keys are out of the scope of Directive. The authors argued that all wallet providers, irrespective of safeguarding private keys, should be out of the scope of AML law since they are, in essence, private transaction providers. "As a private transaction in cash or in vouchers is not subject to AML law, a private transaction in virtual currencies should neither be."

R. Barone and Masciandaro D. compared the money laundering through usury and cryptocurrency obtained through initial coin offering (ICO) [R. Barone and Masciandaro D.,

2019]. After the calibration of the proposed model, the authors stated that money laundering through ICO was not economically profitable.

F. Di Vizio explained the difficulties which faced regulators with the advance of cryptocurrency usage [Di Vizio, F., 2018]. Furthermore, the author presented the evolution of anti-money laundering regulations related to cryptocurrency in Italy. Moreover, he considered the changes that brought the 5th AML EU Directive, 2018 FATF recommendations, and Italian Legislative Decree 125/2019 compared to previous publications. The author explained the laundering opportunities which Bitcoin and ICO could bring to criminals.

Riverditi, M. and Cossavella, G. discussed still controversial nature of bitcoin and its regulation in Italy [Riverditi, M. and Cossavella, G., 2021]. The authors showed that cryptocurrency exchanges should be registered in "Organismo degli Agenti e dei Mediatori" and obliged to profile their customers. They considered the phenomenon of money laundering and the possible usage of FinTech for laundering solutions.

3. Stylized facts of crypto laundering techniques

The money laundering process is usually decomposed into three steps: placement, layering, and integration [Ardizzi et al., 2014].

During the first stage, ill-gotten funds are introduced into the financial system. Crypto exchanges and non-custodial wallet-mixers are used during this step. Still, there are two more steps to be accomplished to protect the identities. Step two is the layering stage. The layering stage's goal is to conceal the origin of "dirty" money. This step usually involves the use of another round of crypto mixers. The third step is the integration step. During the integration step, the aim is to reintroduce the "cleaned" funds into the formal economy. This step involves the use of crypto laundering techniques, such as crypto exchanges, various DeFi projects, and NFT platforms. Below are these crypto-laundering techniques in more detail.

3.1 Cryptocurrency custodial exchanges.

Since the cryptocurrency-related industry is still evolving, the number of exchanges is constantly fluctuating; in September 2021, there were around three hundred exchanges [Coinmarketcap, 2021]. Different types of crypto exchanges exist. This paper examines two types of exchanges: centralized (custodial) and peer-to-peer (non-custodial). Centralized custodial exchanges are "platforms that enable users to buy and sell cryptocurrencies against payment of a fee[6]." These exchanges require full disclosure of the origin of the funds and identifying information. Therefore, these kinds of centralized exchanges are not suitable for crypto laundering (stage one and two), but they are suitable for stage 3 (reintroduction of the funds in the formal economy).

3.2 *Cryptocurrency non-custodial peer-to-peer exchanges*

Non-custodial peer-to-peer exchanges provide a platform maintained and operated by software with no central point of authority, facilitating deals among users by connecting them

[6] Art. 2 (3) lit g Directive 2015/849/EU

to one another[7] without leaving the platform. These kinds of non-custodial exchanges can be used for stages one and two of the money laundering process. Even though they also can be used for stage three, but it will not provide the desired result of cleaned funds.

It is worth mentioning that the use of crypto exchanges has always been a popular crypto-laundering method. Since 2019, the share of illicitly received bitcoins has increased from 30% to 85% [Chainalysis, 2020].

3.3. Non-custodial wallet-mixer

Another category of the popular crypto-laundering method is the use of mixers. Mixers are non-custodial cryptocurrency wallets with the additional function of "mixing" cryptocurrency to conceal the exact origin. A crypto wallet is a service that stores and safeguards cryptocurrency on behalf of customers [Carlo Gola & Andrea Caponera, 2019]. In September 2021, there were at least 84 wallets that differed in functionalities and fees[8]. The main difference of non-custodial wallets, as opposed to custodial form, is the existence of a natural or legal person who takes custody of other people's crypto keys. According to Article 3 (19) Directive 2015/849, a custodial wallet is "an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies." That means that full personal disclosure has to be provided to the custodial wallet platform. Based on that, only non-custodial wallets are suitable for money laundering schemes. These non-custodial wallets are suitable for stages one and two of the crypto laundering process.

3.4. Decentralized Finance (DeFi) projects

The newest technique to launder money is Decentralized Finance (DeFi) projects. These DeFi projects are released through decentralized applications (dApps). Today, most of the DeFi projects run on the Ethereum blockchain. These platforms offer the ability to trade, option for lending, borrowing, or investing in crypto-related products automatically. It is said to be a "global, open alternative to the current financial system.[9]" DeFi is a multi-facet phenomenon that democratizes the financial and financing worlds. However, it opens a grave possibility to launder money quickly and automatically. As an example, a hacker transferred $1 million to "Uniswap" after stealing $200 million from the crypto exchange "KuCoin" [Decrypt, 2020]. DeFi platforms are suitable for the whole scheme money laundering process (stage 1-3), but best they are used for stage three – reintroduction cleaned funds into the formal economy.

3.5. Non-Fungible Token (NFT) platforms

NFT is currently another blockchain-related boom. NFT works as proof of ownership of digital arts in many forms and formats, including images, videos, and music. NFT and their corresponding ownerships are registered in the blockchain, manifesting digital scarcity and uniqueness[10]. Even though the NFT trade is written in the blockchain, involved parties can stay anonymous while using non-custodial wallets. Since NFT can have an agreed value,

[7] Houben, R. and Snyers, A., 2018, pp.77
[8] See https://www.cryptowisser.com/wallets, accessed 01.10.2021
[9] See https://ethereum.org/en/defi/, accessed 01.10.2021
[10] See Kraken Intelligence report, 2021 "Non-Fungible Tokens (NFTs) Redefining Digital Scarcity", accessed 01.10.2021

criminals with ill-gotten cryptocurrencies could use these non-fungible tokes for money laundering purposes, the same as regular art pieces in the real world. NFT platforms are trendy. In September 2021, there were at least sixty-nine NFT platforms.[11] For the first half of 2021, NFT achieved over $927 million in sales [Kraken Intelligence, 2021]. NFT platforms are suitable for stages two and three of the crypto laundering process.

4.Financial Action Task Force (FATF) inter-governmental recommendations

FATF defines a virtual asset as "a digital representation of value that can be digitally traded, or transferred, and can be used for payments or investment purposes" [FATF, 2021]. Cryptocurrencies, DeFi products, and NFT tokens fall under this definition.

FATF also defines virtual asset service providers (VASPs). VASP "means any natural or legal person...conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

1. Exchange between virtual assets and fiat currencies;
2. Exchange between one or more forms of virtual assets;
3. Transfer of virtual assets;
4. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
5. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset" [ibid.].

VASPs are required to be licensed or registered at a minimum in the jurisdiction where they are created [FATFa, 2021]. In addition, VASP should be supervised or monitored by a competent authority. Based on FATF recommendations, VASPs are required to conduct Customer Due Diligence (CDD) when the transaction's threshold is above USD/EUR 1,000 [FATF, 2021]. "Countries should ensure that originating VASPs obtain, and hold required and accurate originator information and required beneficiary information on virtual asset transfers, submit the above information to the beneficiary VASP or financial institution immediately and securely" [ibid].

As seen from the definition of VASPs, all platforms, including DeFi projects and NFT platforms that have a focal point of authority, should be registered and conduct AML/CFT and CDD policies. There is a problem in conducting the AML/CFT and CDD policies based on platforms having or not the central point of authority and custodianship over clients' private information. The non-custodial platforms, where the operators cannot oversee the transactions, do not collect AML/CFT and CDD information.

The following sections look in detail at how Italian regulations and Russian laws address these crypto laundering issues.

[11] See https://sourceforge.net/software/nft/, accessed 01.10.2021

5.Italian regulations against crypto laundering

All member states must follow and transpose the European Union Directives into their national laws in the European Union. These Directives can be furthered in their scopes in the countries' local decrees (laws). Various directives cover money laundering in European Union.

According to Directive (E.U.) 2015/849 of 20 May 2015 (4AML), art.1, par.3, "the following conduct, when committed intentionally, shall be regarded as money laundering:

a. the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;
b. the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;
c. the acquisition, possession or use of property, knowing, at time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;
d. Participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points a, b and c."

In the Italian Republic, the following decrees mandate the money laundering activities: AML/CFT[12] legislation is represented by Decree n. 231 and 109 of 2007 [UIF, 2020] with recent amendments Decree n. 124, 125, and 157 of 2019. Furthermore, Directive (E.U.) 2015/849 of 20 May 2015 (4AML) was transposed into Italian law through Legislative Decree n. 90/2017 of 25 May 2017.

Legislative Decree n. 90/2017 of 25 May 2017 established the definition of virtual currency, highlighting its use as a medium of exchange [Vizio, 2019]. Art. 5, par. I of this Decree categorized entities providing services related to cryptocurrency - as non-financial operators. These entities must comply with AML/CFT policy and must be registered with "Organismo degli Agenti e dei Mediatori" [Riverditi and Cossavella, 2021]. Nevertheless, this Decree was only limited to regulating exchanges between fiat (regular) currency and cryptocurrency. This Decree did not mention nor regulate any services provided by custodial wallet platforms.

On 30 May 2018, new and the most recent, European Directive 2018/843 was passed into law. This Directive represents the fifth Anti-Money Laundering European Directive (5AMLD). According to the 5AMLD, entities that provide exchange services between "virtual currencies" and fiat currencies (art. 1, par. g) and custodial wallet providers (art 1, h) must follow AML/CFT policies. This Directive defined virtual currencies as "a digital

[12] CFT - Countering Terrorist Financing

representation of value that is not issued or guaranteed by a central bank or public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically." Again, it is evident that exchanges trading only cryptocurrency are not included in supervised entities. Also, some DeFi projects and all NFT products being considered not virtual currency are not covered by 5AMLD.

On 4 October 2019, 5AMLD was transposed into the Italian legal system through the Legislative Decree 125/2019 [Gazzeta Ufficiale, 2019]. This Decree furthers the 5AMLD's scope even more: Legislative Decree n. 125/2019 incorporates entities dealing with a digital representation of value, including cryptocurrencies. It covers entities participating in issuing, offering, transferring, and clearing cryptocurrencies (art. 1, par. f). Crypto exchanges, custodial wallets, and DeFi projects fall into this category and must comply with the AML/CFT requirements. According to art.5, par. 1b, custodial crypto platforms are obliged to create a reporting system and communicate potentially suspicious transactions. As we can see, custodial crypto exchanges, custodial wallet providers, and custodial DeFi projects are covered by the latest Decree.

There is an issue in Decree 125/2019 with recognizing NFT transactions. By definition, NFT transactions are not considered involving fiat with cryptocurrency. NFT is not a cryptocurrency by itself because it does not act as a medium of exchange, but only as proof of ownership. Therefore, it does not fall into the scope of regulation. The only time NFT platforms would be considered for AML/CFT requirements is when the NFT platform is custodial, but NFT products by themselves do not fall under the scope of the current regulation.

Non-custodial exchanges also do not fall under the scope of Legislative Decree n. 125. The owners of such platforms do not have custody of the users' information, funds, and private keys. In other words, a non-custodial exchange is a peer-to-peer platform that automatically connects users for an exchange. The non-custodial exchange operates by finding suitable counterparts for the transaction. It means that the cryptocurrency is in the user's wallet until the transaction happens. After the transaction occurs, the cryptocurrency is transferred directly to the other user's wallet. The algorithm is written in such a way that users are matched automatically and instantly. The exchange platforms' owners do not get custody of any funds and are not engaged in any exchange per se. Consequently, these platforms are not in the scope of Legislative Decree n. 125/2019.

Crypto wallets and wallet-mixers could be in custodial and non-custodial forms. According to Legislative Decree n. 125/2019, art. 1, par. g, custodial wallets, which could be mixers, are obliged to follow AML/CFT regulation, and the same does not apply for non-custodial wallets. These non-custodial wallets are being used as the solutions for tumbling cryptocurrencies, i.e., hiding the origin of the funds, therefore, performing the first stage of money laundering. For example, the Wasabi wallet utilized the CoinJoin technique to enhance privacy to camouflage transactions. Cake wallet uses private in-wallet exchanges, therefore, hiding the origin of the funds. These non-custodial wallets are providing the

platforms for stage one of the money laundering operations. These non-custodial wallets are not breaking any laws since they are not required to follow AML/CFT and CDD policy.

To summarize, the Italian regulation successfully confronts crypto laundering through custodial, centralized exchanges, custodial DeFi and NFT platforms, and custodial wallet-mixers. Still, crypto laundering through decentralized non-custodial platforms and NFTs is possible.

6. Russian regulations against crypto laundering

In the Russian Federation, Federal laws are passed in the Parliament (Duma), then approved by Federal Council, and signed by President.

In 2001, Federal Law n. 115-FZ/2001 went into effect, which defined money laundering as follows:

"...bringing a legal appearance to the possession, use or disposal of amounts of money or other property received as the result of committing an offence" [translated by Legislationline, 2021]. This law obliges providers of investment platforms[13], financial platforms,[14]and information systems issuing digital financial assets and exchange providers of digital currency[15], i.e., cryptocurrency, to comply with AML/CFT regulation.

This regulation with amendments covers exchange platforms, DeFi projects, non-fungible tokens (NFTs), and crypto exchange-wallets. Also, it is worth mentioning that Russian Federation only regulates entities and persons within its authority. Any company or natural person registered, located in, or citizen of the Russian Federation falls under its jurisdiction. Any person or entity utilizing the service within the territory of the Russian Federation, using Russian domain names (.ru, .rf) falls under its jurisdiction.

Russia defines crypto exchange as an exchange between any crypto and/or any fiat currencies. Decentralized Finance projects are defined as financial platforms that issue "digital financial assets." NFT platforms are considered as an investment platform issuing "utilitarian digital rights." Wallet providers that only hold cryptocurrency without additional services are not defined or regulated, while wallets providing exchange services are regulated as crypto exchanges. It is also worth mentioning that Russian legislation does not distinguish between custodial and non-custodial service providers. All platforms under Russian regulations being custodial or non-custodial, are obliged to exercise AML/CFT procedures.

According to Federal Law n. 259-FZ of 31.07.2020, "Digital currency is a set of electronic data (digital code or designation) contained in the information system that is offered and/or may be accepted as:

[13] Amended by Federal Law n. 259-FZ of 02.08.2019.
[14] Amended by Federal Law n. 212-FZ of 20.07.2020.
[15] Amended by Federal Law n. 259-FZ of 31.07.2020.

1. A mean of payment that is not the official unit of currency of the Russian Federation, a unit of currency of a foreign country or an international unit of account or currency; and/or
2. An investment in respect of which no person is responsible towards the owners of such electronic data, except for operations and information systems nodes (that are only responsible to ensure the consistency of the issuance of such electronic data and making (amending) entries in such information subject to the rules thereof)" [translated by Buzko R. and Krasnov E., 2021].

According to Federal Law n. 259-FZ of 31.07.2020 art.14, par.2, Russian jurisdiction is applied when cryptocurrency "is deemed issued or exchanged in Russian Federation, if the process involves the use of the Russian information infrastructure objects, including Russian domain names and network addresses or technical infrastructure located in Russian Federation" [translated by Buzko R. and Krasnov E., 2021].

Russian Federation does not distinguish whether the exchange has custodianship. The laws must be followed irrespective of exchanges' type (custodial or non-custodial), the providers must follow AML/CFT policy. If the exchange process takes place not on Russian infrastructures or domains, this exchange is not obliged to comply with AML/CFT rules.

DeFi projects are regulated in Russian Federation as financial platforms. According to Federal Law n.211-FZ of 20.07.2020 art. 2, par.1, "financial platform - information system which provides interaction of the financial organizations or issuers with consumers of financial services by means of the Internet for the purpose of possibility of making of financial transactions and access to which is provided by the operator of financial platform" [translated by CIS-legislation, 2021]. Financial platforms' providers should be legal entities.

DeFi projects use digital financial assets (DFA). According to Federal Law n. 259-FZ of 31.07.2020 art.1, par.2, digital financial assets (DFA) "are a subset of digital rights that are set forth by the decision on the issue of respective DFAs and may include:

a. Monetary claims
b. Ability to exercise rights attaching to issuable securities;
c. Interest in the capital of a non-public joint stock company; and
d. Right to require transfer of issuable securities" [Debevoise & Plimpton, 2020].

DFAs should be issued through a distributed ledger-based information system. As clear from the definition, the DeFi platforms that provide lending, borrowing, and investing services through usage of their tokens, utilize digital financial assets. Therefore, in the case of any DeFi platforms (custodial or non-custodial), their respective administrators should exercise AML/CFT policy.

NFT platforms are considered investment platforms that trade "utilitarian digital rights." According to Federal Law n. 259-FZ of 02.08.2019 art.2, par.1, an "investment platform is the information system on the Internet used for the conclusion by means of information technologies and technical means of this information system of agreements of

investment, access to which is provided by the operator of investment platform" [translated by CIS-legislation, 2021]. On these investment platforms, users can trade "utilitarian digital rights" [translated by Mograbyan, 2020]: "demand the transfer of things or exclusive rights to use them, as well as demand the performance of work and (or) the provision of services." It means that all NFT platforms are considered investment platforms. It also means that non-fungible tokens are, in fact, tradable/exchangeable utilitarian digital rights products. According to this legislation, all NFT platforms and legal entities and natural persons administrating NFT platforms should exercise AML/CFT policy. Yet again, Russian laws do not distinguish between custodial and non-custodial platforms. All platforms, regardless of their custodianship, must comply with AML/CFT procedures if they fall under the jurisdiction of the Russian Federation.

Russian law does not regulate wallet providers as separate entities. Wallets and wallet platforms that provide exchange services are considered as an exchange. Wallets and wallet platforms that only provide the software for storing cryptocurrency are not regulated. Therefore, they are not required to comply with any AML/CFT policy.

It is evident that anti-money laundering regulations in Russian Federation do not differentiate between custodial and non-custodial platforms. All entities involved in the crypto business (such as crypto exchanges, DeFi projects, NFT platforms, and wallets/exchanges) under the jurisdiction of the Russian Federation must comply with the AML/CFT process.

7.Regulation's comparison

Despite significant differences in legal, socio-economic structure, historical and cultural uniqueness, combatting money laundering is a common objective for all governments. However, the approaches are different. The Italian and Russian legislators do not define cryptocurrency in the same manner, and this leads to even more differences in their anti-money laundering regulation related to cryptocurrency. The general economic definition of money is done through its three functions [Von Mises, 2013]: medium of exchange, the standard of deferred payment, and store of value. Even though cryptocurrency is not money, it could operate similarly.

Italian legislation and Russian laws define cryptocurrency in a different manner. Italian government considers cryptocurrency as a medium exchange and a store of value. As per Italian Legislative Decree n. 90/2017 of 25.05.2017 art. 1, par. Qq, cryptocurrency is a digital representation of value, not issued by any Central Bank or public authority, and used as a medium of exchange for goods and services and electronically transferred, archived, and traded. In contrast, the Russian government classifies cryptocurrency as a store of value only. According to Federal Law n. 259-FZ of 31.07.2020 art. 14, par.7, Russian legal entities and natural persons residing in Russian Federation for at least 183 days in consecutive 12 months cannot use cryptocurrency to purchase goods or services. Cryptocurrency can only be used as a store of value for investment purposes and to be exchanged for other cryptocurrencies, digital assets, and utilitarian digital rights. Therefore, in Italy, people can purchase goods and

services, but in Russian Federation, cryptocurrency can only be used as a store of value, i.e., investment tool.

There are also major differences in how DeFi, NFT platforms, crypto exchanges, and crypto wallets are regulated. To summarize, the main difference is in what is being regulated. In the Italian Republic, only custodial platforms being DeFi, exchanges, and wallets are required to comply with AML/CFT policy. At the same time, Non-Fungible tokens (NFTs) are not being considered as a cryptocurrency, do not fall under the existing scheme of Italian regulations.

On the other hand, in the Russian Federation, all custodial and non-custodial platforms being crypto exchanges, DeFi, exchange-wallets, including NFTs, that fall under the authority of the Russian Federation, must exercise AML/CFT policy. Still, it is not clear why regular crypto wallets, that only store crypto, are excluded from the legal consideration in Russian Federation so far.

Like the money laundering process, crypto laundering consists of three steps: placement, layering, and integration.[16] While Russian legislators focus on preventing crypto laundering through the first and the second stages, Italian laws concentrate on preventing crypto laundering through the second and third stages.

8.Case

Let us look at one case of popular non-custodial wallets that DarkNet users in laundering funds are widely using. With this case, we can see how current laws and regulations within the Italian Republic and the Russian Federation are non-effective in stopping it. This is the case of Cake wallet, a legal and fully compliant with current laws crypto exchange wallet.

The information of the widely used Cake wallet was derived from the ClearNet forum that discussed all the cons and pros of illegal activities on the DarkNet.

ClearNet forums are gateways for new and potential DarkNet participants; therefore, we can utilize them to understand the motivations and challenges of these users.[17] The public subreddit r/darknet was chosen for this research project because of its size (184,000 registered members) and the length of time it has been in operation (it was created on December 26, 2009).

We employed the Reddit Scrapper [Agarwal, 2020] to obtain the r/darknet data from the open archive (Pushshift.io, 2021). The data was collected from January 1, 2020, to December 31, 2020. We researched the comments dataset as we were interested in the recommended techniques for exchanging cryptocurrency, but not in the questions per se. The number of comments used for the paper is 189, 256.

[16] More in Section 3.
[17] For more, see our previous work ``The shift of DarkNet illegal drug trade preferences in cryptocurrency: the question of traceability and deterrence"

Aiming to understand the preferred methods of buying and exchanging cryptocurrency, we applied topic models on obtained text data. Then we considered if anti-money laundering regulations covered this method.

Several studies have already utilized ClearNet forums and topic models to determine the effect of DNM busts [Porter, 2018], to discover anomalies signaling the advent of disturbing events [Shah et l., 2019], to determine critical players on specific DNM [Hazel and Shao, 2020].

The usual topic model's approach examines documents over time with different topics, where a topic is a probability distribution over the words [Sohrabi et al., 2018]. The utilization of the Correlation Explanation (CorEx) model allows minimizing starting assumptions and human intervention [Gallagher et al., 2017]. CorEx discovers independent latent factors that explain correlations between observed variables. In this model, X is a group of words, and Y is a topic to be learned. The Total Correlation is zero only when there is no dependence between variables X and Y.

Before analyzing data with CorEx, we removed stop words and punctuation, lowercased data, deleted NaN values, bot entries, and lemmatized text [Spacy.io, 2021]. We defined the stop words like pronouns, swear words, and auxiliary verbs. Moreover, we anonymized the data by removing users' names, identification numbers, and metadata.

Applying the CorEx model in an unsupervised manner without anchor words allowed us to comprehend the most discussed topics every month for 2020.

We chose the topic's number in such a way as to explain 70% of all entries since extra topics contributed only insignificant correlation to the learned models. The data was normalized due to differences in the number of comments per month.

Among the most discussed topics in 2020, we revealed the topic related to the usage of the non-custodial wallet "Cake" wallet (see Appendix A for "Cake wallet" topics over 12 months of 2020).

Since in the realm of DarkNet, the wallets are of interest only as a method to purchase and exchange cryptocurrency in the most untraceable way, and not as the cheapest solution, we hypothesized that these comments were answers to the question of "which wallet is best to use for DarkNet users?" (example Figure 1).

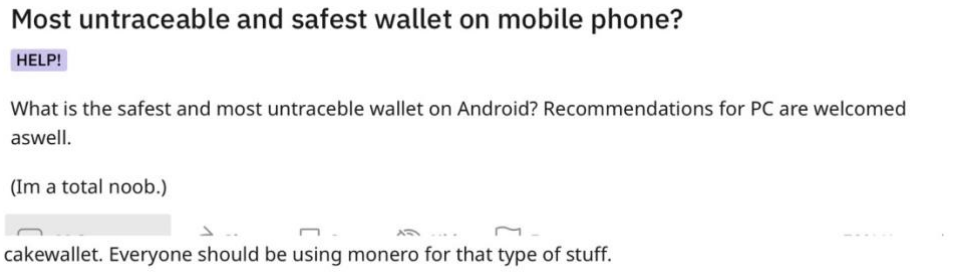

Figure 1. Example of the posts and comments related to the best wallet for buying drugs from DarkNet.

As seen from Figure 2, the discussion of “Cake” had an increasing trend with spikes in May and October 2020. Let us consider what Cake wallet is and why DarkNet users were recommending it.

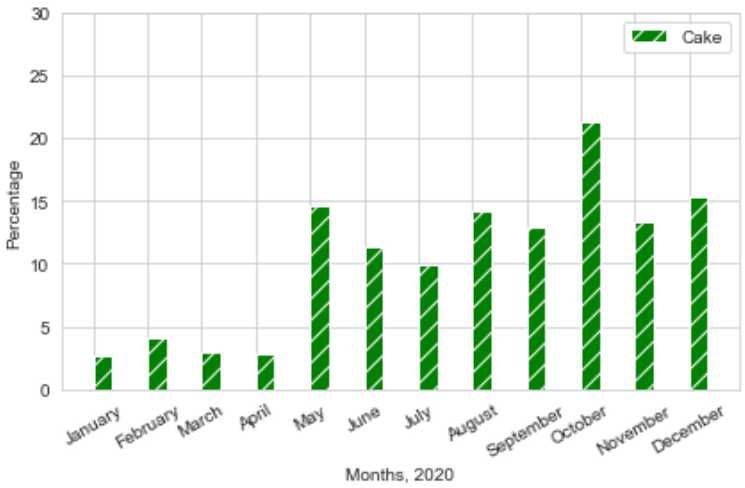

Figure 2. The evolution of “Cake wallet” topic in 2020

The Cake wallet is a non-custodial multicurrency wallet allowing to exchange cryptocurrency directly in the wallet [cakewallet, 2021]. Being open-source, the wallet allows changing the code according to the user's needs. Originally, the Cake wallet was created in 2018 as an open-source Monero wallet, then other cryptocurrencies were added. As we know from our previous work[18], Monero is the preferred cryptocurrency for DarkNet.

Let us consider the Cake wallet in the light of Italian anti-money laundering regulations. Since this wallet is non-custodial, existing decrees do not apply, which explains the wallet's popularity among this specific public.

Considering the Russian regulations, the Cake wallet platform does not have to exercise AML/CFT policies since it is not located in the Russian Federation, is not using Russian infrastructures, and does not hold Russian domain names. Furthermore, since the actual exchanges are performed outside of the scope of Russian jurisdiction, the platform does not have to provide AML/CFT functions even for Russian citizens utilizing its services.

It is evident from the case study that current anti-money laundering laws are outdated and do not cover the activity that DarkNet illegal participants are currently using. The Cake wallet case showed us that only international cooperation and harmonization of anti-money laundering regulation could resolve the problem of money laundering related to cryptocurrency.

9. Limitations of the case study

[18] For more, see our previous work ``The shift of DarkNet illegal drug trade preferences in cryptocurrency: the question of traceability and deterrence”

In the present study, we examined users' comments who presumably buy drugs from the DarkNetMarkets regularly. Although these users wrote that they used Cake wallet regularly, we do not have access to the actual transactions. Therefore, the major limitation is the possible discrepancies between users' words on the forum and the actions.

10. Conclusion

The borderless nature of digital assets and cryptocurrencies creates vast complexity for regulators. Current laws to mandate and govern blockchain-based technologies differ between countries, and these differences in interpretations and requirements allow criminals to be one step ahead. Even though international cooperation between such countries as the Italian Republic and the Russian Federation is done through FATF and other international organizations, these member countries fall behind on their ability to investigate and prevent crypto laundering. One possible solution could be the law harmonization through an international cooperating body.

References:

1. Weimann, G., 2016. Going dark: Terrorism on the dark web. *Studies in Conflict & Terrorism*, *39*(3), pp.195-206.
2. Shillito, M.R., 2019. Untangling the 'Dark Web': an emerging technological challenge for the criminal law. *Information & Communications Technology Law*, *28*(2), pp.186-207.
3. Europol, 2014. "GLOBAL ACTION AGAINST DARK MARKETS ON TOR NET-WORK." https://www.europol.europa.eu/newsroom/news/global-action-against-dark-markets-tor-network (Accessed: 28 September 2021)
4. UNODC, 2021. Money laundering, https://www.unodc.org/unodc/en/money-laundering/overview.html (Accessed: 28 September 2021)
5. FATF, 2012-2021. *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, FATF, Paris, France, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html (Accessed: 28 September 2021)
6. NFTically, 2021, What is NFT (Non-Fungible Token)?, https://help.nftically.com/en/article/what-is-nft-non-fungible-token-1uy0b1h/ (Accessed: 29 September 2021)
7. Coinmarketcap, What is Decentralized Finance? A Deep Dive by the Defiant, https://coinmarketcap.com/alexandria/article/what-is-decentralized-finance (Accessed: 29 September 2021)
8. The New York Times Magazine, 2021. The Untold Story of the NFT Boom, https://www.nytimes.com/2021/05/12/magazine/nft-art-crypto.html (Accessed: 29 September 2021)
9. Walker-Munro, B., 2020. Cyber-Governance, Systemic Governance and Disruption of the Criminal Law. *U. Queensland LJ*, *39*, 225.
10. Adeleke, I., Zubairu, U.M., Abubakar, B., Maitala, F., Mustapha, Y. and Ediuku, E., 2019. A systematic review of cryptocurrency scholarship.

11. Bryans, D., 2014. "Bitcoin and Money Laundering: Mining for an Effective Solution," *Indiana Law Journal*: Vol. 89 : Iss. 1 , Article 13.
Available at: https://www.repository.law.indiana.edu/ilj/vol89/iss1/13
12. Dyntu, V. and Dykyi, O., 2018. Cryptocurrency in the system of money laundering. *Baltic Journal of Economic Studies*, *4*(5), pp.75-81.
13. Frick, T.A, 2019. Virtual and cryptocurrencies—regulatory and anti-money laundering approaches in the European Union and in Switzerland. ERA Forum 20, 99–112. https://doi.org/10.1007/s12027-019-00561-1
14. Campbell-Verduyn, M., 2018. Bitcoin, crypto-coins, and global anti-money laundering governance. Crime Law Soc Change 69, 283–305. https://doi.org/10.1007/s10611-017-9756-5
15. Kinsburskaya V.A., 2019. - Identification of cryptocurrency holders in order to counter the laundering of proceeds from crime and the financing of terrorism // National Security / nota bene.- No. 3. - S. 1 - 14. DOI: 10.7256 / 2454-0668.2019.3.29720 URL: https://nbpublish.com/library_read_article.php? id=29720
16. Haffke, L., Fromberger, M. and Zimmermann, P., 2020. Virtual currencies and anti-money laundering–the shortcomings of the 5th AML Directive (EU) and how to address them. *Journal of Banking Regulation*, pp.125-138.
17. Barone, R. and Masciandaro, D., 2019. Cryptocurrency or usury? Crime and alternative money laundering techniques. *European Journal of Law and Economics*, *47*(2), pp.233-254.
18. Di Vizio, F., 2018. Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti.
19. Riverditi, M. and Cossavella, G. ,2021. 'FinTech: la disciplina penale (limiti e sfide)', *Diritto ed Economia dell'Impresa*, (2), pp. 203–234. Available at: https://search.ebscohost.com/login.aspx?direct=true&db=bsu&AN=151652530&site=ehost-live (Accessed: 30 September 2021).
20. Carlo Gola & Andrea Caponera, 2019. "Policy issues on crypto-assets," LIUC Papers in Economics 2019-7, Cattaneo University (LIUC).
21. Top Cryptocurrency Spot Exchanges, Coinmarketcap, 2021 https://coinmarketcap.com/rankings/exchanges/ (Accessed: 30 September 2021).
22. Houben, R. and Snyers, A., 2018. Cryptocurrencies and blockchain. *Legal context and implications for financial crime, money laundering and tax evasion*.
23. Chu, D., 2018. 'Broker-Dealers for Virtual Currency: Regulating Cryptocurrency Wallets and Exchanges', *Columbia Law Review*, 118(8), pp. 2323–2359. Available at: https://search.ebscohost.com/login.aspx?direct=true&db=bsu&AN=133553682&site=ehost-live (Accessed: 30 September 2021).
24. Gallagher, R.J., Reing, K., Kale, D. and Ver Steeg, G., 2017. Anchored correlation explanation: Topic modeling with minimal domain knowledge. *Transactions of the Association for Computational Linguistics*, *5*, pp.529-542.
25. Porter M., 2018. Analyzing the DarkNetMarkets subreddit for evolutions of tools and trends using LDA topic modeling. Digital Investigation, 26, S87–S97.

26. Shah, D., Hurley, M., Liu, J., & Daggett, M., 2019. Unsupervised content-based characterization and anomaly detection of online community dynamics. In Proceedings of the 52nd Hawaii International Conference on System Sciences.
27. Hazel Kwon, K. and Shao, Chun, 2020. Communicative constitution of illicit online trade collectives: An exploration of darkweb market subreddits. In International Conference on Social Media and Society (pp. 65–72).
28. Agarwal, A., 2020. How to scrape reddit with google scripts. https://www.labnol.org/internet/web-scraping-reddit/28369/. (Accessed: 18 September 2021)
29. Sohrabi, B., Vanani, I. R., & Shineh, M. B., 2018. Topic modeling and classifi- cation of cyberspace papers using text mining. Journal of Cyberspace Studies, 2, 103–125.
30. Gallagher, R. J., Reing, K., Kale, D., and Ver Steeg, G., 2017. Anchored corre- lation explanation: Topic modeling with minimal domain knowledge. Trans- actions of the Association for Computational Linguistics, 5, 529–542.
31. Spacy.io, 2021. Industrial-strength natural language processing. https://spacy.io. (Accessed: 18 September 2021).
32. Legislationline, 2021. Federal Law No. 115-FZ On Countering Money Laundering and the Financing of Terrorism (2001 as amended 2004). https://www.legislationline.org/documents/id/4294 (Accessed: 6 October 2021).
33. CIS-legislation, 2021. FEDERAL LAW OF THE RUSSIAN FEDERATION of August 2, 2019, No. 259-FZ, https://cis-legislation.com/document.fwx?rgn=117701 (Accessed: 6 October 2021).
34. Mograbyan, A., 2021. Digital rights under the civil law of the Russian Federation. In *SHS Web of Conferences* (Vol. 109, p. 01024). EDP Sciences.
35. CIS-legislation, 2021. FEDERAL LAW OF THE RUSSIAN FEDERATION of July 20, 2020 No. 211-FZ, https://cis-legislation.com/document.fwx?rgn=126193 ,(Accessed: 6 October 2021).
36. Debevoise & Plimpton, 2020. Russia Adopts Law on Digital Financial Assets, https://www.debevoise.com/insights/publications/2020/08/russia-adopts-law-on-digital-financial-assets (Accessed: 6 October 2021).
37. Buzko R. and Krasnov E., 2021. Fintech in the Russian Federation: Overview, Practical Law Country Q&A w-014-7425
38. Cakewallet, 2021. https://cakewallet.com/ (Accessed: 9 October 2021).

Appendix A

Month of 2020	Constituents of "Cake wallet" topic
January	transfer,app,coinbase,atm,cake,finally,burner,suspicion,target,morphtoken
February	bitcoin,wallet,monero,tor,noob,vpn,fee,email,extra,cake
March	fee,transaction,atm,coinbase,cake,heroin,arrest,fully,pro,bounce
April	loss,exchange,single,yellow,kraken,mess,interest,cake,official,best
May	electrum,coinbase,fund,kraken,involve,cake,steal,escrow,reporting,content

June	weed,cake,pack,dose,virus,smoke,game,paper,hot,warning
July	monero,bitcoin,wallet,tail,cake,tor,directly,app,security,electrum
August	wallet,monero,bitcoin,government,law,state,cake,enforcement,directly,illegal
September	wallet,cake,transfer,bag,coinbase,kraken,link,electrum,shitty,color
October	pgp,fee,tail,ipsjip,transaction,bomb,cake,app,encryption,exact
November	send,wallet,package,cake,vpn,delivery,android,risk,feature,trouble
December	monero,wallet,bitcoin,tail,cake,buy,tor,fee,anonymous,coinbase