Noziedzīgi iegūtu līdzekļu legalizācijas novēršanas dienests

Office for Prevention of Laundering of Proceeds Derived from Criminal Activity

VIRTUAL CURRENCIES

RISKS OF MONEY LAUNDERING AND FINANCING OF TERRORISM

RIGA

2019

CONTENTS

1. THE NECESSITY FOR RISK ASSESSMENT

1.1. On 23rd of August, 2018, Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (Moneyval) published its Fifth Round Mutual Evaluation Report on Latvia, which details and assesses the measures taken by Latvia in order to prevent money laundering (hereinafter – ML) and terrorism financing (hereinafter – TF) for the reporting period to November 2017.

1.2. Consequently, following the Moneyval report, "Plan of Anti-Money Laundering and Counter-Terrorism Financing Measures for the Period of Time till 31 December 2019" was approved on 11th of October, 2018 with the Cabinet of Ministers Order No 512 (hereinafter – the Plan).[1] The objective of the Plan is to strengthen the capacities of Latvia to combat ML, TF and proliferation and to mitigate the overall ML and TF risks, by ensuring conformity with the international commitments and standards in the field of anti-money laundering (hereinafter – AML) and countering the terrorism financing (hereinafter - CTF) and promoting the public safety, competitiveness of economic environment and confidence in jurisdiction of the Republic of Latvia. The Plan, amongst other, requires the Office for Prevention of Laundering of Proceeds Derived from Criminal Activity (hereinafter - FIU Latvia) to draft a report on the risks of using virtual currency as a new ML/FT method.

1.3. The purpose of this report is to facilitate the awareness of the Latvian AML/CTF policy makers, FIU Latvia, law enforcement agencies, obliged entities under the Law on the Prevention of Money Laundering and Terrorism Financing of the Republic of Latvia, as well as any other interested parties regarding ML and TF risks related to using virtual currencies.

2. RISK ASSESSMENT METHODOLOGY

2.1. This report on ML and TF risks related to using virtual currencies was prepared in accordance with principles of World Bank's methodology.[2]

2.2. FIU Latvia is the responsible authority for the preparation of this report "Virtual currencies: risks of money laundering and financing of terrorism". The information included in this report was summarized and analyzed by the FIU Latvia, in collaboration with the Ministry of Finance of the Republic of Latvia, the State Revenue Service and Latvijas Banka as the co-responsible institutions.

2.3. This report was prepared based on the laws and regulations of the Republic of Latvia, guidelines, studies and opinions prepared by local, as well as EU and international level authorities.

3. VIRTUAL CURRENCIES

3.1. Virtual currencies (hereinafter - VCs), which include cryptocurrencies such as *Bitcoin* or *Ethereum*, as well as a wide range of other digital means of exchange, utilize an innovative new technology that enables digital transactions and the delivery of financial products and services in online networks, environments and marketplaces.

[1] Plan of Anti-Money Laundering and Counter-Terrorism Financing Measures for the Period of Time till 31 December 2019. Available: http://www.fm.gov.lv/en/s/prevention_of_money_laundering_and_terrorism_financing/plan_of_measures_for_mitigation_of_the_money_laundering_and_terrorism_financing_risks_for_2017___2019/

[2] The Word Bank: Risk Assessment Support for Money Laundering/Terrorist Financing. Available: http://www.worldbank.org/en/topic/financialsector/brief/antimoney-laundering-and-combating-the-financing-of-terrorism-risk-assessment-support#1

3.2. Like other financial products and services, VCs have features that present risks for facilitating criminality, including ML and TF. The borderless, peer-to-peer (hereinafter - P2P) nature of certain VCs offers the prospect for potential money launderers and terrorist actors to transfer funds outside the regulated sector and beyond the purview of AML and CTF authorities. VCs also feature varying levels of anonymity and pseudonymity, which can enable the concealment of illicit activity.

3.3. The origin of VCs can be traced back to 2008 and 2009, when an anonymous person or group called "*Satoshi Nakamoto*" created the first decentralized VC, or cryptocurrency, the *Bitcoin*. Much more revolutionary than the cryptocurrency itself, however, was the technology behind it, namely, the *blockchain*, which has been widely discussed since due to the potentially benefits of applying the technology in many other areas. The idea of a network of users that validates transactions through its user collective instead of a middle man (for example, a bank) was groundbreaking. Potentially the technology could facilitate quicker, easier and cheaper transactions compared to traditional means, however, these features are not necessarily achieved now due to scalability, energy consumption and other issues that *Bitcoin* or the *blockchain* presents. The technology is not limited to VCs, but can work for almost every type of transaction between parties.[3]

3.4. Essentially, with *blockchain*, the information of a transaction is stored in a data block. In this block, users solve arithmetical problem underlying a transaction (mining) and distribute it within the network. If the majority of the network approves such a solution (proof-of-work), the new block is connected to the previous block via a cryptographic step, a unique thumbprint (hash). This creates a chain of transaction blocks that is further supplemented using the same approach and this chain is referred to as the *blockchain*. All blocks are publicly accessible in a decentralized register (ledger) and distributed to all members of the network (P2P structure). Due to the uniqueness of each hash and the publicity of the ledger, the *blockchain* is extremely secure against manipulation.

3.5. It should be noted that *Bitcoin* is not perfectly anonymous, but rather pseudonymous, because sending and receiving of *Bitcoins* is carried out under pseudonyms (cryptographic addresses) of both counterparties involved in the transaction. In the ecosystem of *Bitcoin*, addresses are not tied to the identity of the persons. However, every *Bitcoin* transaction is stored for an unlimited period of time in the *blockchain* that is publicly visible.

3.6. Other VCs, such as *Monero*, *Dash*, and *Zcash*, are different from *Bitcoin* in a way that they offer the option of private transactions (anonymity) and are not visible. Due to the described anonymity favoring features described above, VCs do not fit well into the traditional financial system in which banks and other institutions are subject to increasingly strict Know Your Customer requirements, which restrict banking secrecy.[4]

3.7. The Financial Action Task Force (hereinafter - FATF) took up the specific topic of VCs when it published its report on VCs and related ML/TF risks thereof.[5] The mentioned report suggests that VCs' global accessibility allows them to exist in a digital universe outside the reach of any particular country. Furthermore, the report describes VCs as being particularly vulnerable to anonymity risks because customer identification features such as name and address are not attached to a user's details, as well as because the system has no central service provider that has oversight of transactions and which could be held accountable.

3.8. Following the increased popularity of VCs and the related risks mentioned above, the European Union (hereinafter – the EU) regards mitigating the ML and TF risks associated with VCs as a significant security priority. The EU adopted Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (hereinafter - 5AMLD), which requires that EU member states bring VC exchange platforms and custodial wallet providers within the scope of their AML/CFT regulations. This marks an important step in bringing transparency to VC networks across the EU and is consistent with guidance issued by the FATF.

---

[3] Directorate General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs. Study "Virtual currencies and terrorist financing: assessing the risks and evaluating responses". Available: http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf

[4] Policy Department for Economic, Scientific and Quality of Life Policies; author: Kiel Institute for the World Economy Directorate-General for Internal Policies: Virtual Currencies - Monetary Dialogue July 2018. Available: http://www.europarl.europa.eu/cmsdata/149902/KIEL_FINAL%20publication.pdf

[5] Financial Action Task Force, Virtual Currencies: Key Definitions and Potential AML/CFT Risks, FATF Report, Paris, June 2014. Available: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potentialaml-cft-risks.pdf.

4. LEGAL FRAMEWORK OF VIRTUAL CURRENCIES IN THE EU

4.1. Back in 2012, the European Central Bank (hereinafter - ECB) released a report on VC schemes wherein the ECB addressed the issue of accelerating proliferation of cryptocurrencies, as well as the effects of this proliferation on the economy and on the reputation of Central Banks in Europe. This study done by the ECB is the very first time an EU institution acknowledged cryptocurrencies in any formal manner and, simultaneously, it was the first attempt at their legal categorization and definition.[6]

4.2. The definition of VCs set out in the ECB's report was constructed with a specific purpose in mind, which was to cover all the potential uses of VCs. In a following opinion published in 2016, the ECB pointed out three possible problems with this broad definition, namely, VCs do not qualify as currencies from EU perspective; consequently, it would be more accurate to regard them as a means of exchange, rather than as a means of payment; and that the proposed definition does not take into account that in some circumstances VCs can be used for purposes other than that of a means of payment. As VCs lack the key attributes of sovereign currencies, in order not to associate VCs with money or currency, the ECB promotes the usage of term "crypto-asset" could be used instead. At the same time the FATF promotes the usage of term "virtual-asset".[7]

4.3. In 2014, the European Banking Authority (hereinafter - EBA) published its opinion on VCs, where it defines VCs as a digital representation of value that is neither issued by a central bank or public authority, nor necessarily attached to a legal tender. VCs are accepted by natural or legal persons as a means of payment and can be transferred, stored or traded.[8]

4.4. The most noteworthy call to action regarding VC regulation on the supranational level came about on 5th of July, 2016, when the European Commission published its proposal to amend the Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (hereinafter – 4AMLD). In the text of the proposal to amend the 4AMLD, the Commission identified that there are existing gaps in the oversight of the many financial means used by terrorists, from cash and trade in cultural artifacts to VCs and anonymous pre-paid cards.

4.5. According to the European Commission, the biggest issue is that VCs can be utilized by and terrorist organizations to carry out anonymous transactions, allowing them to fund their operations without being discovered by the authorities.[9] The same can be regarded to money launderers. As mentioned, the 5AMLD brings cryptocurrency exchanges and custodian wallet providers under the scope of AML and CTF regulations. This means that they must register with the AML authority in the respective jurisdiction, and implement necessary customer due diligence processes, monitor transactions, report suspicious activity, etc. The 5AMLD also provides the definitions of VCs and VC exchanges and custodian wallet providers in line with the FATF's guidelines[10].

4.6. The 5AMLD defines VC exchanges as "providers engaged in exchange services between virtual currencies and fiat currencies" and custodian wallet providers as "entity that provides services

[6] European Central Bank: Virtual currency schemes. Available: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf
[7] Financial Action Task Force, publication "Regulation of virtual assets". Available: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html
[8] European Banking Authority: Opinion on 'virtual currencies'. Available: https://eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf
[9] Policy Department for Economic, Scientific and Quality of Life Policies; Authors: Prof. Dr. Robby HOUBEN, Alexander SNYERS "Cryptocurrencies and *blockchain*: Legal context and implications for financial crime, money laundering and tax evasion". Available: http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf
[10] Financial Action Task Force, Virtual Currencies: Key Definitions and Potential AML/CFT Risks, FATF Report, Paris, June 2014. Available: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potentialaml-cft-risks.pdf.

to safeguard private cryptographic keys on behalf of their customers, to hold, store and transfer virtual currencies."[11]

4.7. VCs are defined as follows: "means a digital representation of value that is not issued or guaranteed by a central bank or a 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."[12]

4.8. As soon as the 5AMLD is incorporated into the national legislation of EU member states – VC exchanges and custodians will have to register with the relevant AML authority in their jurisdiction, identify users, monitor transactions, report suspicious activity, and give national investigators greater access to information.

5. LEGAL FRAMEWORK OF VIRTUAL CURRENCIES IN LATVIA

5.1. With amendments to the Law on the Prevention of Money Laundering and Terrorism Financing (hereinafter – AML/CTF Law) of 26th of October, 2017, the article 1 of the respective law was supplemented with definitions of VCs and VC service providers. The definition of VCs is as follows: "a digital representation of the value which can be transferred, stored or traded digitally and operate as a means of exchange, but has not been recognized as a legal means of payment, cannot be recognized as a banknote and coin, non-cash money and electronic money, and is not a monetary value accrued in the payment instrument which is used in the cases referred to in Section 3 Clauses 10 and 11 of the Law on the Payment Services and Electronic Money" and VC service providers are defined as "person providing virtual currency services, including the provider of services of exchange of the virtual currency issued by other persons, which provides the users with the possibility to exchange the virtual currency for another virtual currency by receiving commission for it, or offer to purchase and redeem the virtual currency through a recognized legal means of payment".

5.2. Furthermore, the respective amendments to the AML/CTF Law stipulate that VC service providers shall be obliged entities under the AML/CTF Law, which is in line with the requirements of 5AMLD. Therefore, as of 1st of July 2019, a provision of the AML/CTF Law sets into force, set out in point 17 of the transitional provisions thereof, providing that VC service providers will become the obliged entities under the Latvian AML/CTF Law and their supervisory authority will be the State Revenue Service.[13] Additionally, in accordance with the requirements of the 5AMLD, the FIU Latvia shall have the rights to access the VC wallets of natural and legal persons.

5.3. The 5AMLD must be transposed to the local legislation until 10th of January, 2020. It should be noted that in order to fully transpose the 5AMLD in the local legislation, the AML/CTF Law requires to be supplemented with a provision which determines also custodian wallet providers as obliged entities under the respective law.

5.4. However, the mentioned amendments of AML/CTF Law are a step ahead of 5AMLD stipulating that also virtual currency converters shall be obliged entities under the AML/CTF Law.

5.5. Although, it is clear that the above described regulations would provide stricter AML/CTF requirements for the VC service providers and enable the supervisory processes thereof, additional registration and licensing requirements should be set up. Amendments to the AML/CTF Law set out minimum requirements in Article 10^1 (i.e. the minimum to be met, by the adequacy

[11] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU - Article 1. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843

[12] Financial Action Task Force, Virtual Currencies: Key Definitions and Potential AML/CFT Risks, FATF Report, Paris, June 2014. Available: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potentialaml-cft-risks.pdf.

[13] Law on the Prevention of Money Laundering and Terrorism Financing. Latvijas Vēstnesis, 116 (3900), 30.07.2008.; Latvijas Republikas Saeimas un Ministru Kabineta Ziņotājs, 16, 28.08.2008. – Article 45, Part two (version as of 1st of July, 2019).

of the staff responsible for fulfilling the requirements of the AML/CFT Law, including senior management). Such requirements should be supplemented with additional limitations, e.g., a prohibition to take the position of chairman of the board, a person responsible for the enforcement of AML/CTF requirements, etc., if the candidate of taking such a position in the VC service provider, does not have an impeccable reputation, or the person has been convicted of an intentional criminal offense.

6. INHERENT VULNERABILITIES AND ML/TF THREATS RELATED TO VIRTUAL CURRENCIES

6.1. A study prepared by the European Parliament "Cryptocurrencies and *blockchain*: Legal context and implications for financial crime, money laundering and tax evasion" provides information that the illustrative is that the total market capitalization of the 100 largest cryptocurrencies (VCs) is reported to exceed the equivalent of 330 billion euros globally by early 2018.[14] However, taking into account that at the end of 2017 *Bitcoin* was at its peak value, as well as considering the fact that *Bitcoin* is the cryptocurrency with by far the highest market cap, the estimated capitalization as of today is significantly smaller – around 155 billion euros[15].

6.2. Ministry of Finance of the Republic of Latvia in its informative report regarding VCs, indicated that precise data on the use of VCs among the population of the EU are not available, however, data from surveys of activity of VC exchange platforms allow to estimate that the volume of VCs used in the EU and, especially in Latvia, is insignificant compared to the value of euro payments.[16]

6.3. However, the "National Money Laundering Risk Assessment 2018" prepared by the U.S. Department of the Treasury, specifies that global ML syndicates have added the option of moving illicit proceeds into and through VCs as another way to layer transactions in order to hide the origin of illicit funds.[17] Furthermore, a study has found that illegal activity accounts for a sizable proportion of the users and trading activity in *Bitcoin*, as well as an economically meaningful amount in dollar terms. For example, approximately one quarter of all *Bitcoin* users and close to one-half of transactions thereof are associated with illegal activity.[18] In the light of the foregoing, it appears that VCs are used as a tool to move illicit funds within the U.S. rather than the within the EU. However, this may also be an indicator that the EU lacks resources to identify such movement of illicit funds.

6.4. According to the European Commission, as well as other, publicly available sources[19], the most significant threat related to VCs is associated with the fact that most VC transactions cannot be linked to identified persons, namely, the anonymity and pseudonymity characteristics of VCs (including the *non-face-to-face* characteristics). Another feature of VCs that may hold some appeal for terrorist actors or money-launderers is the ability to enable value transfers of VCs internationally whilst avoiding regulated intermediaries. Although, VC (e.g. *Bitcoin*) transactions offer a level of anonymity similar to cash transactions, unlike a cash transaction, which is strictly

---

[14] Policy Department for Economic, Scientific and Quality of Life Policies; Authors: Prof. Dr. Robby HOUBEN, Alexander SNYERS "Cryptocurrencies and *blockchain*: Legal context and implications for financial crime, money laundering and tax evasion". Available: http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

[15] Unofficial data source on VC market capitalization: "Top 100 Cryptocurrencies by Market Capitalization". Available: https://coinmarketcap.com/

[16] Ministry of Finance of the Republic of Latvia: Informative Report on The benefits and risks of using Virtual Currencies and the actions to develop areas and reduce identified risks

[17] U.S. Department of the Treasury. "National Money Laundering Risk Assessment 2018". Available: https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf

[18] Foley, Sean and Karlsen, Jonathan R. and Putnins, Talis J., Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? (December 14, 2018). Review of Financial Studies, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3102645

[19] For example, see: U.S. Department of the Treasury. "Risks and Vulnerabilities of Virtual Currency", 2017. Available: https://www.dni.gov/files/PE/Documents/9---2017-AEP_Risks-and-Vulnerabilities-of-Virtual-Currency.pdf

private between entities, a VC transaction with anonymous *Bitcoin* addressees is recorded on a publicly visible, distributed electronic ledger. Additionally, the possibility to enable value transfers of VCs internationally with a level of anonymity may hold appeal to persons with intentions related to bribery and corruption. However, most likely due to the fact that VCs do hold a possibility to be tracked to some extent, there have not been any cases of bribery or corruption involving VCs identified.

6.5. It should be added that the 2017 Internet Organised Crime Threat Assessment (IOCTA) published by the European Union Agency for Law Enforcement Cooperation (Europol) indicates that VCs might not yet be the most favored means used for the purposes of ML, as the assessment states that cash continues to play an important role when it comes to criminals realizing their criminal gains; it has well-established methodologies for laundering, and is as readily exchangeable, relatively untraceable, and pseudo-anonymous – similar to the cryptocurrencies favored in the digital underground. Therefore VCs have yet to be adopted to any large degree by established money launderers who are likely to favor long established methodologies.[20]

6.6. In its 2014 opinion[21], the EBA emphasized 5 (five) ML or TF risks and 9 (nine) financial crime risks related to VCs, most of which were rated as being high. The ML or TF risks listed thereof are as follows:

6.6.1. Criminals are able to launder proceeds of crime because they can deposit/transfer VCs anonymously;
6.6.2. Criminals are able to launder proceeds of crime because they can deposit/transfer VCs globally, rapidly and irrevocably;
6.6.3. Criminals/terrorists can use the VC remittance systems and accounts for financing purposes;
6.6.4. Criminals/terrorists can disguise the origins of criminal proceeds, undermining the ability of enforcement to obtain evidence and recover criminal assets;
6.6.5. Market participants can be controlled by criminals, terrorists or related organizations.

6.7. It should be taken into account that the above listed risks were identified by EBA in 2014, when *Bitcoin* and other VCs gained their popularity in a world-wide level. Since that time, the society and most notably – law enforcement agencies and FIUs have gained understanding and experience related to VCs. Consequently, following the increase in knowledge of obliged entities, as well as the law enforcement, many of the risks identified in 2014, today might not appear as significant ML or TF risks. However, it should be noted that since 2014, the amount, value and popularity in usage of VCs has grown, therefore making the above listed risks even greater. For example, the first of the above listed risks – the anonymity of VCs still is considered the main risk related to VCs in connection with ML or TF, however, as described above, a positive feature in cases of some VCs (e.g. *Bitcoin*, *Ethereum*) is that there is a possibility to trace the flow of VCs.[22] Most risks identified above correspond not only to VCs, but also fiat money, including non-cash means (for example, the risk identified by EBA listed as No 5).

6.8. In addition, international investigations, especially those involving advanced technology, can create challenges for law enforcement with respect to gathering evidence and information.[23] The uncertain or non-existing legal instruments to trace, freeze and seize illicit VCs or VCs that are related to illicit funds, can create an obstacle for law enforcement. In Latvia, there have been several criminal cases related to VCs, investigated by the State Police, as well as State Revenue Service. The investigated cases thereof include purchases in black markets, such as *Darkweb*, and also cases where fraud using VCs has been identified. Experts, including law enforcement, have stated that transactions with *Bitcoin* can be traced without any excessive challenges[24]. Also the legal framework for arrest of VCs can be considered comprehensive, namely, VCs are arrested and, if necessary, stored and preserved as any other object. However, the application of legal framework for tracing, gathering evidence, freezing and seizure of VCs may require interpretation.

6.9. Summing up the aforementioned arguments, the potential of VC involvement in ML or TF should not be underestimated. Even though most VCs leave a digital footprint, it might, in some cases, be challenging if not impossible to link the digital footprint to a physical person, especially if a

[20] European Union Agency for Law Enforcement Cooperation (Europol): 2017 Internet Organised Crime Threat Assessment (IOCTA). Available: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017
[21] European Banking Authority: Opinion on 'virtual currencies'. Available: https://eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf
[22] There are platforms that allow any person to follow transactions of VCs. For example, please see: https://www.blockchain.com/explorer. Furthermore, outsourcing of *blockchain* know-your-transactions services are available. For example, see https://www.chainalysis.com/ or https://www.neutrino.nu/.
[23] U.S. Department of the Treasury. "National Money Laundering Risk Assessment 2018". Available: https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf
[24] Please see: "*Latvijā saistībā ar kriptovalūtām sākti vairāki krimināprocesi*". Available: https://www.tvnet.lv/4521970/latvija-saistiba-ar-kriptovalutam-sakti-vairaki-kriminalprocesi

person has extensive knowledge regarding covering the connection between the two (hiding IP, bypassing regulated exchanges, etc.). Also the lack of finalized legal framework should be stressed. Therefore, the legal framework governing the use of such instruments should be customized also to be applied in cases where VCs are involved. Meanwhile, guidelines for law enforcement regarding actions that should be carried out in situations, where illicit VCs have been identified, should be drafted in order to successfully fight against ML and TF, where VCs are used.

6.10. Another, less discussed, ML related scenario, would be that instead of using fiat money (convention currencies), which is potentially derived from criminal activity, to directly purchase VCs, the same funds could be used to purchase computer-related hardware to start a VC mining operation. As this computer-related hardware would earn VCs (e.g. *Bitcoin*) through the mining process. However, in order to successfully engage in profitable mining process, it most likely will require large investments as well as energy and time consuming process.

6.11. As mentioned before, the EBA also emphasized nine financial crime risks related to VCs. The most noteworthy of financial crime risks identified by EBA are as follows:

6.11.1. Criminals can use VCs to trade illegal commodities, such as drugs and weapons;
6.11.2. Criminal organizations can use VCs to settle internal or inter-organizational payments;
6.11.3. Hacking of VC software, wallets or exchanges allows a criminal to implicate others in the criminal activities they commit;
6.11.4. Criminals can create challenges for seizure of assets, confiscation, embargos and identifying the avoidance of financial sanctions;
6.11.5. Tax evaders are able to obtain income in VCs.

6.12. As described above, many of the ML and TF related risks identified in 2014, as of today are no longer considered to be as significant as they were in 2014. However, financial crime risks listed above continue to rise concerns in relation to the usage of VCs. Based on the above described risks identified by EBA, it appears that VCs are most likely to be used in criminal activities related to financial crime, rather than ML, TF or bribery and corruption.

6.13. In light of the foregoing considerations and based on currently available information on the volumes of VCs used in the EU and Latvia, VCs currently do not create systemic risks for Latvia's payment system and financial stability. [25]

7. INHERENT VULNERABILITIES AND ML/TF THREATS RELATED TO INITIAL COIN OFFERINGS

7.1. In the recent years, there has been a new phenomenon, which goes hand to hand with VCs, for companies to attract capital from investors through so-called Initial Coin Offerings (hereinafter - ICOs). ICOs are a type of crowdfunding where the company sells newly issued VCs, or tokens, typically to raise funds in the form of other VCs, which the company can then exchange for fiat money to fund its operations (the use of *Ethereum* has been a particularly popular vehicle for ICOs). The tokens issued by such a company are typically either supposed to be used in the future as the means of exchange for services on a platform the company seeks to develop (so called utility tokens), be a VC (VC tokens), or represent some equity adjacent investment in a company (securities tokens). In simple terms, an ICO takes one asset (namely, a VC, e.g.

[25] Ministry of Finance of the Republic of Latvia: Informative Report on The benefits and risks of using Virtual Currencies and the actions to develop areas and reduce identified risks

Ethereum) and exchanges it for newly issued token. These new tokens can further be freely transferred or traded for other VCs or fiat money on cryptocurrency exchanges worldwide.

7.2. Therefore, it is consequent that ICOs might be vulnerable to ML and TF risks due to the anonymity favoring nature of the transactions, and the ease with which large sums of funds may be raised in a short period of time and further exchanged to any other VC or fiat money. By redeeming VC for tokens, ICO issuers are potentially exchanging VC that originated from illicit activity for newly issued tokens that can then be sold for euros or other conventional currencies.

7.3. The Financial and Capital Market Commission (hereinafter – the FCMC) has published an explanation[26] on the possibilities of using VCs and ICOs and the applicable regulations thereof, providing the FCMC's opinion on transactions with VCs in relation with ICOs. The explanation also provides guidance with relation to AML and CTF requirements. In essence, the respective explanation sets out instructions regarding the applicable legal framework for ICOs and provides guidance regarding cases when different types of ICOs fall under licensing requirements.

7.4. Ministry of Finance of the Republic of Latvia in its informative report regarding VCs stressed that currently there still are types of ICOs that are not covered by legal regulation, however, the lack of legal framework identified thereof is related to other risks rather than ML and TF related risks.[27] The risks related to ICOs that are identified in the mentioned report are, e.g., risk of currency exchange failure, financial pyramid risk, risk of fraud, etc. Notwithstanding the listed risks, ML and TF related risks should also be addressed and assessed. In cases of ICOs, increased attention should be paid to the source of the raised funds. However, the ML and TF related risks in respect of the capital attracted trough ICOs appears to be similar as in cases of any other crowdfunding process.

8. RISK MITIGATION MEASURES

8.1. In most of the cases where fiat money is exchanged for VCs (VC is purchased) or vice versa, involvement of financial institutions is required[28] (apart from cases when VCs are exchanged to other VCs or tokens, cases of VC mining operations, or individuals exchanging cash for VCs). The process how fiat money is exchanged into VC, in simple terms, is as follows:

8.1.1. Fiat money is deposited in to an account held in an financial institution;
8.1.2. The respective funds are virtually transferred from the account held in a financial institution to an account held in VC exchange (hereinafter - VCE);
8.1.3. The respective funds are transferred to an account held in VCE are converted into VC and available for use in a virtual wallet.

8.2. Consequently, financial institutions monitor businesses with VC related transactions as the financial institutions monitor other high-risk businesses. Specific risk-based approach for VC related transactions should be applied. This includes that financial institutions should understand customer's motivation and the business rationale for carrying out VC related transactions in order for the financial institution to be able to further apply the risk-based approach.

8.3. Specific elements to consider when applying risk based approach include, but are not limited to: lack of clear business rationale for purchasing VCs; higher-risk convertible VCs used to exchange fiat currency (e.g. *Monero*, *Dash*, *Zcash*); etc.[29]

---

[26] The Financial and Capital Market Commission "Explanation on the possibilities of using the VCs and ICOs and the applicable regulations thereof". Available: http://www.fktk.lv/attachments/article/7435/ICO_skaidrojums_23012019.pdf

[27] Ministry of Finance of the Republic of Latvia: Informative Report on The benefits and risks of using Virtual Currencies and the actions to develop areas and reduce identified risks

[28] FATF in its 2018 report on "Professional Money Laundering" provided the following typology for ML related to VCs: Money launderers arrange schemes that allow criminals to cash out proceeds generated in VC via online illicit markets (e.g. *Darkweb*). In many cases, payments for illicit drugs purchased online are transferred to electronic wallets. Afterwards, VC is transferred through a complex chain of electronic wallets, which may include the use of mixer services. Funds are then sent back to the electronic wallet of the criminal, and subsequently transferred to bank cards and withdrawn in cash. Consequently, also in the provided scenario the services of financial institution are required. For more information, please see: http://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf

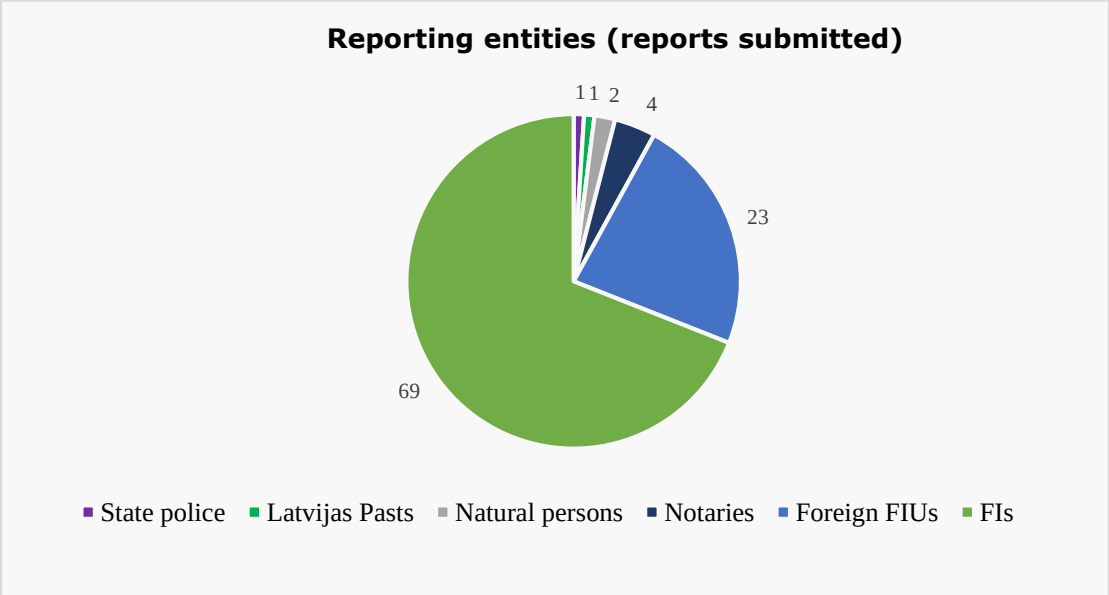
[29] For additional elements, see: Financial Action Task Force "Guidance for a risk-based approach virtual currencies". Available: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

8.4. In 2017 the Finance Latvia Association published Policy and guidelines for AML and CTF and sanctions compliance (the document was updated on 2018), which state that entities that use electronic money or VCs as in their core business, pose disproportionate risk to the financial sector of Latvia.[30] Such a statement is based on a fact that the mentioned entities mainly rely on the internal controls of financial institutions. In respect to the mentioned guidelines, a number of credit institutions do not commence business relationship with clients – entities that use electronic money or VCs as in their core business. Such an approach mitigates the risk to be involved in ML or TF related to VCs. Nevertheless it shall be noted that contrary to VCs, the issuance of electronic money and provision of electronic money transfers are licensed activities regulated by the Law on Payment Services and Electronic Money ensuring full traceability of persons involved in e-money transactions at the same level of transparency as for non-cash transactions using bank deposits.

9. STATISTICS AND EXAMPLES FROM FIU LATVIA

9.1. Notwithstanding to the fact that VCs have gained popularity in the recent years, since the beginning of VCs in late 2008, the FIU Latvia has received only approximately 100 reports[31] that are related to VCs, first report thereof was received on 2011. A vast majority of the reports, namely 49 reports, were received during 2018.

9.2. These 100 reports have been submitted by the State Police of Latvia, Foreign FIUs[32], notaries, financial institutions and natural persons (bank employees) and "Latvijas Pasts" JSC (main postal service provider of the Republic of Latvia).



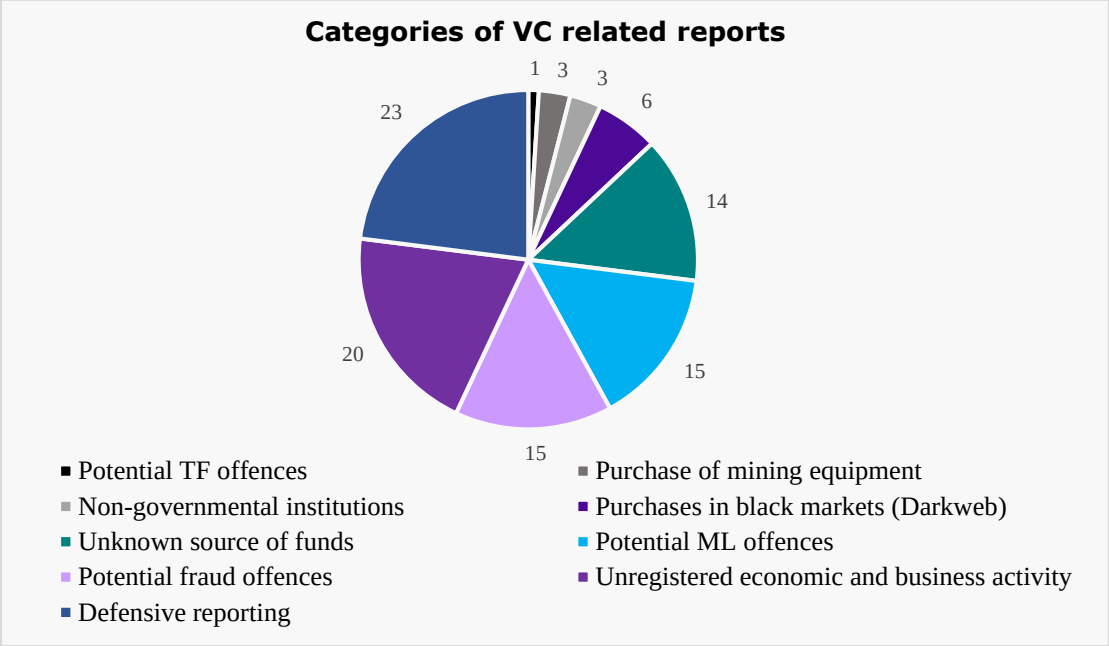
9.3. In the context of the considerations set out in this report, the above mentioned reports related to VCs can be split into several different categories, namely, reports related to:

1. purchase of mining equipment;
2. potential ML offences;

[30] Finance Latvia Association: "Policy and Guidelines for anti-money laundering and counter terrorism financing and sanctions compliance". Available: https://www.financelatvia.eu/wp-content/uploads/2018/12/LV_final_16112018.pdf
[31] Exact amount of reports related to VCs received by the FIU Latvia cannot be identified due to the fact that there is no common element or keyword to identify reports thereof. The statistics were prepared based on several keywords selected by the FIU Latvia (including names of VCs). The total amount of VC related reports identified was 101 (one hundred and one), one of which involved an entity related to VCs, however, the report itself had no relation to VCs. Therefore, the sample reviewed is 100 (one hundred) reports.
[32] Reports have been received from FIUs from the following countries: Czech Republic, Finland, France, Germany, Lithuania, Luxembourg, the Netherlands, Norway, Slovakia, Spain, and the United Kingdom.

3. potential TF offences;
4. potential fraud offences;
5. non-governmental institutions;
6. purchases in black markets (*Darkweb*);
7. unregistered economic and business activity;
8. unknown source of funds;
9. defensive reporting.

9.4. Almost one quarter of all reports can be considered as defensive reports. In these cases, the reporting entities have submitted reports mainly due to the lack of knowledge and understanding of VCs. Example includes cases when the report is submitted regarding an ordinary purchase of VC (e.g. *Bitcoin* purchased via *Coinbase*[33]). One-fifth of all VC related reports are connected with unregistered economic and business activities, where the reporting entity identifies that a person is carrying out continuous transactions with VCs, although the respective person has not registered such a business activity or even is a natural person not carrying out any economic or business activity. Also fifteen cases related to potential financial pyramids or fraud had been reported and fifteen cases of potential ML offences. Examples of reports related to potential ML offences include cases where VC are issued as loans (or vice versa), purchases of real estate, as well as VCs being exchanged to other commodities. Also reports regarding unknown source of funds have been submitted, as well as reports regarding transactions connected to purchases in black markets (*Darkweb*). There have been three reports regarding sale or purchase of VC mining equipment. However, only one report related to TF has been identified.



9.5. Out of the above listed 100 reports, 8 have been escalated to cases, first of which was identified in 2014. Two cases related to VCs and which amount to comparably large values are the following:

9.5.1. As a result of phishing, small amounts of funds had been defrauded from several persons (summing up a larger amount of funds) from two jurisdictions - Austria and Germany. The defrauded funds were transferred to a single bank account, where they were later used to purchase *Bitcoin*.

9.5.2. As a result of fraud, using the persons trust, a person of an older age was misled to exchange a real estate for VCs (which, as a result of investigation, appeared not to have any further use, namely, it was a financial pyramid).

9.6. Although the numbers of VC related reports are low[34], this does not necessarily indicate that VCs are not a threat to ML or TF. The insignificant number of cases related to VCs could potentially be an indicator that the anonymity favoring feature of VCs is hindering the possibility for the obliged entities under the AML/CTF Law to report any such information.

[33] *Coinbase* is a well-known digital currency wallet and platform where merchants and consumers can transact with VCs like *Bitcoin*, *Ethereum* and *Litecoin*. Please see: https://www.coinbase.com/about
[34] The FIU Latvia received the total 34597 reports within 2018 and only approximately 49 were related to VCs.

10. SUMMARY

10.1. In light of the foregoing considerations, the FIU Latvia acknowledges the inherent vulnerabilities, as well as ML and TF risks associated with VCs and the risk level thereof is rated as **High**.

10.2. The risk level is determined taking into account the currently available information on the volumes of VCs used in the EU and Latvia (although precise data on the use of VCs are not available), which is also confirmed with the statistics of reports related to VCs received by the FIU Latvia. Notwithstanding the mentioned, FIU Latvia recognizes that the insignificant number of reports related to VCs might demonstrate problem with identification of VC transaction related to ML and TF.

10.3. The main ML and TF risks associated with VCs identified in this report are related to the anonymity and global transferability favoring features of VCs, as well as the lack of regulation thereof.

10.4. At the time when VC service providers become obliged entities under the AML/CTF Law, Financial institutions, as well as other obliged entities under the AML/CTF Law, which do commence business relationship with entities that use VCs (including VC service providers) as a part of their business (as well as in any other situation, where VCs are involved), should apply the risk-based approach described by the FATF, namely, understanding that the risks related to one or another VC are different – VCs with more anonymity favoring features, such as *Monero* or *Dash*, pose higher ML/TF risks that other VCs[35], e.g., *Bitcoin* – VCs that are based on *blockchain* technology**.** However, in any case, persons actively conducting transactions with VCs should be considered of high risk.

[35] Policy Department for Economic, Scientific and Quality of Life Policies; Authors: Prof. Dr. Robby HOUBEN, Alexander SNYERS "Cryptocurrencies and *blockchain*: Legal context and implications for financial crime, money laundering and tax evasion". Available: http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

11. BIBLIOGRAPHY

Laws and regulations

1. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU - Article 1. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843
2. Law on the Prevention of Money Laundering and Terrorism Financing. Latvijas Vēstnesis, 116 (3900), 30.07.2008.; Latvijas Republikas Saeimas un Ministru Kabineta Ziņotājs, 16, 28.08.2008. – Article 45, Part two (version as of 1st of July, 2019).
3. Plan of Anti-Money Laundering and Counter-Terrorism Financing Measures for the Period of Time till 31 December 2019. Available: http://www.fm.gov.lv/en/s/prevention_of_money_laundering_and_terrorism_financing/plan_of_measures_for_mitigation_of_the_money_laundering_and_terrorism_financing_risks_for_2017__2019/

Other sources

1. Directorate General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs. Study "Virtual currencies and terrorist financing: assessing the risks and evaluating responses". Available: http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf
2. European Central Bank: Virtual currency schemes. Available: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf
3. European Banking Authority: Opinion on 'virtual currencies'. Available: https://eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf
4. European Union Agency for Law Enforcement Cooperation (Europol): 2017 Internet Organised Crime Threat Assessment (IOCTA). Available: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017
5. Finance Latvia Association: "Policy and Guidelines for anti-money laundering and counter terrorism financing and sanctions compliance". Available: https://www.financelatvia.eu/wp-content/uploads/2018/12/LV_final_16112018.pdf
6. Ministry of Finance of the Republic of Latvia: "Informative Report on The benefits and risks of using Virtual Currencies and the actions to develop areas and reduce identified risks"
7. Policy Department for Economic, Scientific and Quality of Life Policies; author: Kiel Institute for the World Economy Directorate-General for Internal Policies: Virtual Currencies - Monetary Dialogue July 2018. Available: http://www.europarl.europa.eu/cmsdata/149902/KIEL_FINAL%20publication.pdf
8. Policy Department for Economic, Scientific and Quality of Life Policies; Authors: Prof. Dr. Robby HOUBEN, Alexander SNYERS "Cryptocurrencies and *blockchain*: Legal context and implications for financial crime, money laundering and tax evasion". Available: http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf
9. The Financial and Capital Market Commission "Explanation on the possibilities of using the VCs and ICOs and the applicable regulations thereof". Available: http://www.fktk.lv/attachments/article/7435/ICO_skaidrojums_23012019.pdf
10. The Financial Action Task Force "Guidance for a risk-based approach virtual currencies". Available: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf
11. The Financial Action Task Force, publication "Regulation of virtual assets". Available: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html
12. The Financial Action Task Force, Virtual Currencies: Key Definitions and Potential AML/CFT Risks, FATF Report, Paris, June 2014. Available: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potentialaml-cft-risks.pdf.
13. U.S. Department of the Treasury. "Risks and Vulnerabilities of Virtual Currency", 2017. Available: https://www.dni.gov/files/PE/Documents/9---2017-AEP_Risks-and-Vulnerabilities-of-Virtual-Currency.pdf
14. U.S. Department of the Treasury. "National Money Laundering Risk Assessment 2018". Available: https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf

15. The Word Bank: Risk Assessment Support for Money Laundering/Terrorist Financing. Available: http://www.worldbank.org/en/topic/financialsector/brief/antimoney-laundering-and-combating-the-financing-of-terrorism-risk-assessment-support#1
16. "*Latvijā saistībā ar kriptovalūtām sākti vairāki krimināprocesi*". Available: https://www.tvnet.lv/4521970/latvija-saistiba-ar-kriptovalutam-sakti-vairaki-kriminalprocesi