



Financial Intelligence  
Unit

# Virtual Assets: Money Laundering and Terrorism and Proliferation Financing Risk Assessment

---

2022



## Table of Contents

<b>I. INTRODUCTION.....</b>	<b>2</b>
<b>II. REGULATORY FRAMEWORK.....</b>	<b>3</b>
1. Latvian legislation.....	3
2. Legislative framework in Estonia and Lithuania .....	3
3. EU legislation .....	4
<b>III. GLOBAL TRENDS IN THE INDUSTRY OF VIRTUAL ASSETS.....</b>	<b>5</b>
1. Implementation of FATF standards .....	5
2. Research on the use of virtual assets in crime .....	5
3. NFTs.....	6
4. Sanctions.....	7
<b>IV. THE SITUATION IN LATVIA.....</b>	<b>8</b>
1. Identification of VASPs.....	8
2. Suspicious transaction reporting and financial intelligence .....	8
3. Investigations.....	9
<b>V. CONCLUSIONS .....</b>	<b>12</b>
<b>ABBREVIATIONS AND TERMS .....</b>	<b>13</b>

## I. INTRODUCTION

1. New technologies, products and related services are creating new opportunities for criminals and terrorists to launder their proceeds and finance illicit activities. Similarly, the lack of a common understanding and knowledge of emerging technologies among the authorities regarding the ML/TF/PF prevention system only increases the risks of ML/TF/PF. A risk-based approach is therefore particularly relevant in the context of emerging technologies. It is essential to inform public and private sector authorities about new risks (including emerging technologies) and their management to ensure that risks are managed and mitigated appropriately<sup>1</sup>.
2. One of the FIU's tasks is to produce a National ML/TF/PF Risk Assessment Report, where the assessment period and frequency of the last two reports have been three and four years respectively. However, since 2019, the FIU has conducted an annual assessment of emerging technologies (including emerging *threats*) and related ML/TF/PF risks. This is largely due to the growing relevance of a particular "emerging technology" - virtual assets. The use of virtual assets in crime is not slowing down, and is introducing new trends. The obligation to prepare this Risk Assessment is enshrined in paragraph 1.2 of the Action Plan.
3. The Risk Assessment has been prepared as a supplement and update to the 2021 version – VCRA 2021. As discussed further in the document, the regulatory framework specified in the AML/CFT Law and licensing in the area of virtual assets in Latvia has not changed in the past year. Consequently, the situation in the sector of virtual assets has not changed, and the FIU's handling of suspicious transaction reports and law enforcement investigations remains similarly typological and problematic.
4. The ML/TF/PF risks posed by virtual assets have remained unchanged since the development of the VCRA 2021 and are therefore not reiterated in this document. Newly identified ML risks relate to the discussed recent developments in the industry of virtual assets and are mentioned in the relevant subsections of Chapter III.
5. The Risk Assessment has been developed by the FIU, analysing the information at its disposal, studies developed by international organisations, as well as using information prepared specifically for the Risk Assessment by the MoF, SRS, SP CPD and FCMC.
6. Given that the terms cryptocurrencies and virtual currencies are used synonymously in various sources, this Risk Assessment also uses both terms. In this document the terms "virtual currency" and "virtual assets" in some cases are used interchangeably based on the corresponding source.

<sup>1</sup> Updated guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers. Available: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>

## II. REGULATORY FRAMEWORK

### 1. Latvian legislation

7. Since the VCRA 2021<sup>2</sup>, the regulatory framework in Latvia has not changed, so there is still a need for a comprehensive regulation of virtual assets (currencies, NFTs, tokens). Based on the information provided by the MoF, by 01.07.2023 it is envisaged to develop the regulation of virtual assets, adapted to the requirements of the EU regulatory framework and FATF standards in the area of regulation of virtual assets. The inclusion of a code for virtual asset service providers in the NACE Rev.2 classification is also intended within this deadline, in order to identify and account for economic activities related to virtual assets.
8. As regards the regulation (and supervision) of virtual assets and their service providers, international standards allow for both registration and licensing mechanisms. According to the supervisory and control body for VASPs, the SRS, the most appropriate mechanism is licensing. At the same time, this view is also supported by industry representatives, for whom a licence or state-issued permission to carry out a specific economic activity would facilitate potential cooperation with credit institutions and other business partners. A detailed description of these issues is included in the VCRA 2021.
9. Similarly, financial policy makers' near-term plans include the task of strengthening the supervision of certain sectors of the obliged entities of the AML/CFT Law, in particular in the area of emerging technologies. This objective is also to be reinforced in the Action Plan, which will include the responsibilities and tasks of the competent authorities for the prevention of ML/TF/PF in the period from 2023 to 2025.

### 2. Legislative framework in Estonia and Lithuania

10. Estonia is one of the first countries in Europe to develop appropriate regulation and issue licences for VASPs, already in 2017. Licences are issued by the Estonian FIU, which also performs the ML/TF/PF prevention supervisory function for VASPs. Initially, the requirements for obtaining a licence were relatively low, and it was possible to license companies that were not operating in Estonia or had no connection with it at all. The number of licence applications increased rapidly, with four licences issued in 2017, rising to 599 in 2018 and 1 234 in 2019. Many of these companies had no direct link to Estonia. This created a very high risk of criminal use of this licensing mechanism. Nor was effective monitoring possible under such a system<sup>3</sup>.
11. At the end of 2021, the head of the Estonian FIU expressed an opinion that licences already issued to VASPs should be revoked and "reissued". Given that the risks of crime in virtual environments are very high and not fully understood by society, the response must be swift and radical. In 2020, the Estonian FIU revoked 1808 licences of VASPs and by October 2021 there were only 400 such licences in Estonia<sup>4</sup>.
12. On 15 March 2022, amendments to the Estonian Anti-Money Laundering and Anti-Terrorist Financing Act entered into force, which supplemented and modified the existing procedure and requirements for obtaining a licence for VASPs<sup>5</sup>. One of the main objectives of the regulatory changes was to mitigate the ML, TF and PF risks in the area of virtual assets.
13. The main change was the additional criteria for obtaining a licence as a VASP:
  - 13.1. the share capital of the virtual currency exchange service provider must be at least EUR 100,000 or EUR 250,000 if it (also) provides a virtual currency transfer service;

<sup>2</sup> Virtual currencies: money laundering and terrorism and proliferation financing risk assessment.

Available in Latvian:

[https://fid.gov.lv/uploads/files/2021/virtu%C4%81l%C4%81s%20val%C5%ABtas/FID\\_VV%20risku%20nov%C4%93rt%C4%93jums.pdf](https://fid.gov.lv/uploads/files/2021/virtu%C4%81l%C4%81s%20val%C5%ABtas/FID_VV%20risku%20nov%C4%93rt%C4%93jums.pdf)

Available in English:

<https://fid.gov.lv/uploads/files/2021/virtu%C4%81l%C4%81s%20val%C5%ABtas/VIRTUAL%20CURRENCIES.pdf>

<sup>3</sup> Why were new rules necessary? Available:

<https://www.fin.ee/en/faq-how-will-new-estonian-draft-legislation-affect-virtual-assets-and-crypto#why-were-new-rules-n>

<sup>4</sup> Estonian Financial Watchdog Calls to Revoke Crypto Businesses Licenses. Available:

<https://www.financemagnates.com/cryptocurrency/regulation/estonian-financial-watchdog-calls-to-revoke-crypto-businesses-licenses/>

<sup>5</sup> Guidelines for submission of an application for the authorisation of a VASP or an application for amendment of the authorisation. Available:

<https://fiu.ee/en/guidelines-fiu/guidelines#guidelines-for-submi-2>

- 13.2. prerequisites for customer identification and research;
  - 13.3. the VASP must submit a business plan;
  - 13.4. specific equity capital requirements at any point in the life of the VASP;
  - 13.5. a mandatory requirement for an audit organised by the VASP;
  - 13.6. requirements relating to the VASP's actual location and the board members' education, professional experience, membership on the boards of other companies.<sup>6</sup>
14. The Lithuanian legal framework is more similar to the situation in Latvia. In Lithuania, VASPs (virtual currency exchanges and/or virtual currency wallet operators) are also not licensed. However, it is mandatory to inform the Lithuanian Register of Companies within five working days of the commencement or termination of such activity. As in Latvia, such registration with the Register of Companies imposes an obligation to comply with the legislation on the prevention of ML, TF and PF.<sup>7</sup>
15. The Lithuanian Financial Crime Investigation Service (FIU equivalent) is the supervisory authority for the prevention of ML/TF/PF of VASPs. The staff of its ML Prevention Office provides methodological assistance to responsible entities in the implementation of ML prevention measures.
16. Lithuania is currently witnessing a very rapid increase in the number of companies operating in the virtual asset space. Eight new VASPs were registered in 2020, and 188 in 2021. More than 40 such companies were registered in the first few months of the year 2022. According to the Lithuanian Register of Enterprises, there were 252 VASPs operating in Lithuania in March 2022. However, it should be noted that, as in Latvia, virtual assets are not recognised as legal tender in Lithuania and are not expected to become so in the foreseeable future.<sup>8</sup>

### 3. EU legislation

17. At the EU level, work has been underway since Q3 2020 on the MiCA single framework<sup>9</sup>, which will replace national regulations on virtual assets once it is developed. This will require national regulation to transpose the scope and requirements of the MiCA Regulation. The MiCA regulation will provisionally enter into force in 2025.
18. New regulation of virtual assets:
- 18.1. will promote legal certainty for virtual assets that are not covered by existing EU financial services legislation and for which there is now a clear need;
  - 18.2. set common rules at EU level for providers and issuers of virtual assets and cryptocurrencies
  - 18.3. will replace EU Member States' existing laws that apply to virtual assets not covered by existing EU financial services legislation;
  - 18.4. set specific rules for the use and maintenance of the so-called stable cryptocurrency, or *stablecoin*.
19. As the FCMC has pointed out, the MiCA framework will foster cooperation between countries, provide greater regulatory certainty for market participants engaged in cross-border activities and help further innovation and consumer choice in financial services. The new regulation of virtual assets will help ensure a high level of consumer and investor protection, market integrity and financial stability by applying ML prevention requirements to the relationships between participants involved in virtual asset transactions.

<sup>6</sup> Guidelines for submission of an application for the authorisation of a VASP or an application for amendment of the authorisation. Available: <https://fiu.ee/en/guidelines-fiu/guidelines#guidelines-for-submi-2>

<sup>7</sup> Information for legal entities carrying out the activities of virtual currency exchange operators and (or) depository virtual currency wallet operators in the republic of Lithuania. Financial Crime Investigation Service. Available: <https://www.fntt.lt/en/money-laundering-prevention/information-for-legal-entities-carrying-out-the-activities-of-virtual-currency-exchange-operators-and-or-depository-virtual-currency-wallet-operators-in-the-republic-of-lithuania/4115>

<sup>8</sup> Elliptic Connect summary for Lithuania. Available: <https://hub.elliptic.co/country-guides/lithuania/>

<sup>9</sup> Proposal for a Regulation of the European Parliament and of the Council on markets in cryptoassets. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593>

### III. GLOBAL TRENDS IN THE INDUSTRY OF VIRTUAL ASSETS

#### 1. Implementation of FATF standards

20. In June 2022, an update to the FATF's *Targeted Update on Implementation of FATF's Standards on VAs and VASPs* was published<sup>10</sup>. The report builds on previous versions of FATF material and focuses in particular on the disclosure obligations of both the originator and the recipient of a cryptocurrency transfer (*travel rule*).
21. The paper finds that many countries still need to strengthen their understanding of the risks of ML/TF in virtual asset transactions and the VASP sector, and that jurisdictions have made very little progress in implementing FATF Recommendation 15 and its interpretative note (R.15/INR.15) over the past year.
22. The FATF report highlights that technological solutions are now available to facilitate compliance with the *travel rule* in practice, but that the private sector needs to continue to work on issues of interoperability (between different solutions and different jurisdictions) and work towards full compliance with international standards.
23. The FATF stresses the urgent need for countries to accelerate the introduction of appropriate regulation of virtual assets and VASPs to reduce their criminal and terrorist use.
24. It should also be mentioned that the main ML/TF risks for virtual assets identified by the FATF and mentioned in the VCRA 2021 have not lost their relevance in the last year. The main trends remain:
  - 24.1. Most of the identified cases of ML and TF related to virtual assets take place in the virtual asset environment from the outset, i.e., the proceeds of crime are obtained in the form of virtual assets from the outset (e.g., crypto-ransomware payments in virtual assets, *Darknet* payments in virtual assets, investment fraud, etc.).
  - 24.2. Virtual assets are used, among other things, to commit the following crimes: ML, sale of narcotic drugs, psychotropic substances and other prohibited goods and substances (including firearms), fraud, tax evasion, sanctions violations, computer crime (e.g., cyber-attacks resulting in theft or involving ransomware), child exploitation, human trafficking and TF. Fraud (such as investment fraud and extortion) and drug-related offences are the most common.

#### 2. Research on the use of virtual assets in crime

25. In February 2022, blockchain data platform Chainalysis published an extensive study on the use of cryptocurrencies in crime<sup>11</sup>. Chainalysis estimates the criminal share of all cryptocurrency transactions in 2021 at 0.15%. In 2020, this indicator had been higher at 0.62% and in 2019, the share of criminal assets in cryptocurrency transactions had reached an all-time high of 3.37%<sup>12</sup>. According to Chainalysis itself, this figure for 2021 is still subject to change and may have already been revised since February.
26. At the same time, the European Central Bank has very different assessments of the criminal part of cryptocurrency transactions. In his speech in April 2022, Fabio Panetta, Member of the Executive Board of the European Central Bank, said that "Crypto-assets are widely used for criminal and terrorist activities. It is estimated that the amounts of crypto-assets exchanged for criminal purposes are substantial, exceeding USD 24 billion in 2021. Research suggests that as much as USD 72 billion per year, or about 23% of all transactions, is associated with criminal activities."<sup>13</sup>
27. In the absence of a common methodology (or understanding) for calculating such indicators, and given the limited access to relevant data (even more so for more specific indicators), it is virtually impossible to know the current situation in the sector of virtual assets (including its involvement in crime). This makes it difficult to identify specific ML/TF/PF risks and could potentially present a risk in itself.

<sup>10</sup> Targeted Update on Implementation of FATF's Standards on VAs and VASPs. Available:

<https://www.fatf-gafi.org/publications/fatfrecommendations/documents/targeted-update-virtual-assets-vasps.html>

<sup>11</sup> The 2022 Crypto Crime Report, Available: <https://go.chainalysis.com/2022-Crypto-Crime-Report.html>

<sup>12</sup> The 2022 Crypto Crime Report, p. 4. Available: <https://go.chainalysis.com/2022-Crypto-Crime-Report.html>

<sup>13</sup> <https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220425~6436006db0.en.html>

28. Criminals using cryptocurrencies have at least one common goal: to move the proceeds of crime so that they are hidden from surveillance and law enforcement authorities and ultimately "safely" converted into *fiat* currency. Consequently, ML is one of the main criminal offences in the environment of virtual assets, with the proceeds of crime generated in the traditional financial system or immediately in virtual assets (e.g., drug trafficking, kidnap ransom demand, child pornography, etc.). Most of the cryptocurrencies moved between illegal addresses end up in the surprisingly narrow hands of service providers who, based on an analysis of their transactions, appear to be specifically designed for the purposes of ML.<sup>14</sup>
29. The use of DeFi (*decentralised finance*) smart contracts (Chainalysis document - *DeFi protocols*) in the ML virtual environment grew rapidly in 2021. Since 2018, centralised virtual asset exchanges have received the majority of transactions made by criminal virtual asset addresses. However, by 2021, this ratio has fallen significantly to 47%, largely due to the takeover of this role by DeFi smart contracts. They account for 17% of all funds sent from criminal virtual wallets. A year earlier, only 2% of all criminal transactions were diverted to DeFi smart contracts<sup>15</sup>.
30. DeFi is an automated and decentralised digital infrastructure comprising virtual assets, trade finance instruments, loans and other financial services. Unlike traditional finance, DeFi is a marketplace where services are based on programmed *smart contracts* that automate transactions based on predefined, pre-programmed conditions. These conditions are publicly available and replace a centralised service provider or managing authority. Market participants can connect to service providers to lend, borrow or receive other services. Since 2019, the value included in the DeFi market has grown from €2.2 billion to €12.7 billion in 2022.<sup>16</sup>
31. The DeFi market involves a number of ML risks. The risks are related to the fact that DeFi markets have the characteristics of virtual assets, which include the possibility of automating their operation in a smart contract. Criminals can set up DeFi services (long and complex transaction schemes, making it very difficult to trace funds) that automatically transfer virtual assets to other linked wallets, with the aim of obfuscating the origin of funds. Unregulated financial services can be used as fictitious instruments for storing money, and criminals can be assured of the safety of their funds.

### 3. NFTs

32. NFTs are unique digital certificates written on a blockchain and linked to a specific digital object.<sup>17</sup> Most often, this digital link confirms ownership of digital or physical assets such as images, videos, audio files or other property. Such NFT functions are managed through smart contracts and digital wallets. As these activities are recorded in the blockchain, they are publicly verifiable and auditable.
33. The NFT market has developed and continues to develop at a rapid pace in recent years. As of 2019, nearly USD 41 billion worth of cryptocurrency had been tracked in NFT transactions on just one blockchain protocol.<sup>18</sup> Although NFTs are based on the same blockchain technology as virtual currencies, NFTs differ in that the value of tokens cannot be substituted by one another.
34. Many of the risks of ML related to virtual currencies<sup>19</sup> are also specific to the fast-growing segment of NFTs, which are virtually exempt from customer identification and due diligence and transaction monitoring requirements. NFTs are also characterised by the risks of ML inherent in high-value goods (e.g., works of art). The absence of customer identification and due diligence requirements creates increased risks of ML/TF/PF for the users of these platforms and for the integrity of the financial system as a whole.
35. The FIU has developed an ML/TF/PF risk assessment which assesses the risks arising from the use of NFTs. Given the rapid development and growing popularity of NFTs, the FIU considers it particularly

<sup>14</sup> The 2022 Crypto Crime Report, p. 10. Available: <https://go.chainalysis.com/2022-Crypto-Crime-Report.html>

<sup>15</sup> The 2022 Crypto Crime Report, p. 11-12. Available: <https://go.chainalysis.com/2022-Crypto-Crime-Report.html>

<sup>16</sup> Global Financial Stability Report, Chapter 3 - The Rapid Growth of Fintech: Vulnerabilities and Challenges for Financial Stability. Available: <https://www.imf.org/-/media/Files/Publications/GFSR/2022/April/English/ch3.ashx>

<sup>17</sup> NFTs are mainly characterised by three features: 1) they represent a unique object that can be clearly linked to the digital wallet; 2) they are not reproducible or interchangeable; 3) they cannot be divided into parts. See "What You Need to Know About Non-Fungible Tokens (NFTs)". Available: <https://www.forbes.com/uk/advisor/investing/nftnon-fungible-token/>

<sup>18</sup> Crime and NFTs: Chainalysis Detects Significant Wash Trading and Some NFT Money Laundering In this Emerging Asset Class. Available: <https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-nft-wash-trading-money-laundering/>

<sup>19</sup> See VCRA 2021. Available: <https://fid.gov.lv/uploads/files/2021/virtu%C4%81%C4%81s%20val%C5%ABtas/FIDVV%20risku%20nov%C4%93rt%C4%93jums.pdf>

important to anticipate trends in ML/TF/PF and assess the risks associated with this virtual solution. The NFT risk assessment is available on the FIU website in both English and Latvian.<sup>20</sup>

#### 4. Sanctions

36. The use of virtual assets to circumvent, violate or attempt to circumvent sanctions is seen as one possible means of doing so, on a par with other financial products or services. The same applies to VASPs - they can be used (knowingly or unknowingly) to circumvent sanctions. For example, the *Kraken* US cryptocurrency exchange is suspected of violating US sanctions against Iran and is under federal investigation for this alleged violation. It is worrying in this respect that *Kraken's* CEO said that "Defaulting to the law is not advisable, but it should always be considered as an option."<sup>21</sup>
37. In order to ensure a common understanding of the application of sanctions and to capture typologies and indicators of attempts to circumvent sanctions, in March 2022 FIU established a Sanctions Working Group, which brought together experts from FIU, the Prosecutor's Office of the Republic of Latvia, the State Security Service, the Financial and Capital Market Commission, the State Revenue Service and five Latvian credit institutions. The Working Group produced and published a material titled "Indicators of sanctions evasion against Russia".<sup>22</sup>
28. The material defines two indicators that implicate the use of virtual assets and that may be indicative of sanctions evasion or attempted sanctions evasion:
  - 28.1. After the entry into force of the sanctions against Russia, a person directly or indirectly linked to the subject of the sanctions conducts uncharacteristic transactions in virtual assets, including involving virtual assets of dubious reputation, VASPs, cryptocurrency mixers.
  - 28.2. Following the entry into force of the sanctions against Russia, customers are being asked to settle payments for services/goods provided by a sanctioned entity to accounts in other countries, in particular neighbouring countries of Russia, or jurisdictions that do not impose sanctions against Russia; customers are also encouraged to settle payments using less traceable, or monitorable, payment methods (e.g., virtual currencies).

<sup>20</sup> Money Laundering, Terrorism and Proliferation Financing Risks of NFTs. Available: [https://fid.gov.lv/uploads/files/2022/AMLIH/FIU\\_MLTPF%20risks%20of%20NFTs.pdf](https://fid.gov.lv/uploads/files/2022/AMLIH/FIU_MLTPF%20risks%20of%20NFTs.pdf)

<sup>21</sup> Kraken, a U.S. Crypto Exchange, Is Suspected of Violating Sanctions, The New York Times. Available: <https://www-nytimes-com.cdn.ampproject.org/c/s/www.nytimes.com/2022/07/26/technology/kraken-crypto-iran.amp.html>

<sup>22</sup> Indicators of sanctions evasion against Russia. Available: [https://fid.gov.lv/uploads/files/2022/sankcijas/ENG\\_sankcijas\\_ES\\_Clean\\_28072022.pdf](https://fid.gov.lv/uploads/files/2022/sankcijas/ENG_sankcijas_ES_Clean_28072022.pdf)



## IV. THE SITUATION IN LATVIA

### 1. Identification of VASPs

39. In 2022, 10 legal entities registered as VASPs are under the supervision of the SRS. In 2021, there were only 7, compared to 4 the year before.
40. Among the VASPs that the FIU was able to contact, there was one that had already disclosed last year that it did not provide virtual asset services, and one that is no longer in business and is in the process of liquidation. Therefore, the actual number of registered VASPs in Latvia is less than 10.
41. As part of the Risk Assessment, the FIU organised meetings with 4 VASPs. All of the currency service providers met reiterated the need for a licensing mechanism, previously reported in last year's Risk Assessment. These legal entities face a number of challenges - restrictions on providing services abroad, restrictions on finding business partners, restrictions on advertising their activities, etc.
42. The reluctance of Latvian credit institutions to open current accounts for VASPs was also a recurring problem at these meetings. It is positive that at least one service provider has managed to open an account with a Latvian credit institution. VASPs are aware of the high risks in the sector and the cost of managing them, but in addition, they cite a possible lack of understanding of virtual asset services, the specifics of their operations and the possibilities for monitoring transactions as reasons for not opening accounts.
43. A lack of common understanding has also been identified in some cases with regard to the definition of VASPs, their level of risk, blockchain technology as such, etc. In addition, there are divergent perceptions among VASPs themselves, public authorities and other market participants (such as credit institutions).

### 2. Suspicious transaction reporting and financial intelligence

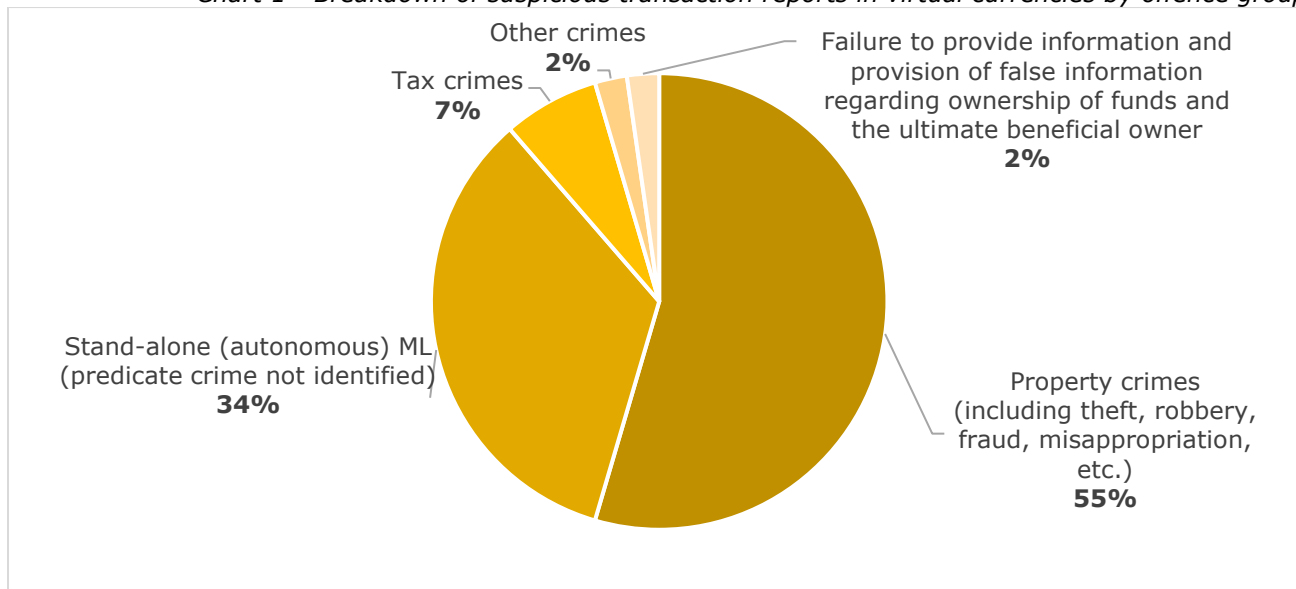
44. In the second half of 2022, no suspicious transaction reports from VASPs have yet been received by the FIU. The number of VASPs is small, but continues to grow slightly, and VASPs have been subject to the AML/CFT Law for more than three years (since 1 July 2019).
45. One VASP submitted a threshold declaration in November 2021 for the case "Customer makes a cash transaction equivalent to €7,000 or more". As VASPs do not provide payment services within the meaning of the Payment Services and Electronic Money Act, they are not required to make cash or other threshold declarations.<sup>23</sup> In the opinion of the FIU, however, the legislation should set a threshold for virtual asset transactions above which the AML/CFT Law obliged entity would be required to make a threshold declaration to the FIU. Such a proposal, together with other options for improving legislation, has already been included in VCRA 2021.
46. During the 9-month period (1 October 2021 to 30 June 2022), 43 suspicious transaction reports were received with the indicator "Customer makes suspicious transactions with virtual currencies" selected. 42 of these reports were issued by 4 different credit institutions, which is to be considered both in terms of the share of the sector in the total number of reports and in terms of the type and content of the alleged offences. In addition, one of these reports was a notice of refraining from executing a transaction, which the FIU had found to be in line with the AML/CFT Law and had temporarily frozen.<sup>24</sup>
47. The total value of these reports is €7.9 million and they include more than 2,000 transactions. On average, the value of a single report is EUR 188 000 and the average number of transactions is 49.

<sup>23</sup> Cabinet Regulation No 550 "Regulations on the procedure and content of suspicious transaction reports and threshold declarations", point 14.1. Available: <https://likumi.lv/ta/id/325463-noteikumi-par-aizdomigu-darījumu-zinojumu-un-slieksna-deklarācijas-iesniegšanas-kartību-un-saturu>

<sup>24</sup> Since 1 October 2021, the FIU has implemented and is working within the new goAML reporting system. The system developed new and improved existing typologies and indicators to better prioritise, group and analyse suspicious transaction reports. Among others, a new indicator "Customer makes suspicious transactions with virtual currencies (T15)" was introduced, which should be manually ticked by the obliged entity when reporting suspicious transactions, if necessary. Previously, in order to identify the number of reports involving virtual currencies, key words associated with virtual currencies were searched, thus selecting messages that mention virtual currencies in any way or context. Changes to the reporting system and, consequently, the methodology for selecting reports are the reason for the apparent decrease in the number of reports in virtual currencies. This is partly because obliged entities do not always tick the relevant indicator, but also because some of the reports identified above did not always contain transactions in virtual currencies and mentioned virtual currencies in an oblique way.

48. The potential offence groups identified in these reports are very similar to those identified in the previous Risk Assessment period. In the majority of cases (55% or 24 reports), these are property crimes (including fraud, which underlies these reports); in 34% or 15 reports, the predicate offence has not been identified and there are autonomous features of ML. 7%, or 3 reports, raised suspicions of tax offences.

Chart 1 - Breakdown of suspicious transaction reports in virtual currencies by offence group



49. The majority of the reports where the offence group is property crime (17 out of 24 reports) also include the report indicator of "Credit institution reports fraud equivalent to less than the total of 50 minimum monthly salaries". It is also interesting to note that 14 virtual currency reports have been flagged for information to be provided to the SRS (in these cases, the information is also automatically sent to the SRS), although only three reports have raised suspicions of tax offences.
50. The most common typologies mentioned in virtual currency reports are "Origin of funds and/or the economic rationale of the transactions is not clear as customer does not provide an explanation or provides a hard-to-verify explanation" and "Customer or other person reports a possible criminal offence". The typology "Customer's account is controlled by a third party and there are suspicions that actions have been taken to conceal or disguise the true ownership of the funds" appears slightly less frequently, but repeatedly (6 reports).
51. Both the offence groups and the typologies indicated and the additional offence of fraud not exceeding 50 minimum monthly salaries are considered appropriate given the content of the reports:
- 51.1. Around half of the reports identify a credit institution customer as a victim of fraud where virtual currency has been used to purchase funds. There are cases where the customer has bought cryptocurrencies on their own, believing the fraudsters' promises, and cases where the customer was unaware that their online banking details had been accessed by a third party.
- 51.2. The other half of the reports identifies suspicious transactions with virtual currencies in the customer's account. These include suspected fictitious transactions by the customer, untraceable virtual currency transactions, NFT transactions at inappropriate market prices, transit account features (the customer is a potential fraudster or money mule) and others.

### 3. Investigations


52. In line with the recommendations of the European Commission's draft Structural Reform Support Programme to increase the capacity of the Central Criminal Police, changes to the functions and structure have been made as of 1 July 2022 and have entered into force as of 1 August this year. As part of the reforms, a new unit has been created - the Cybercrime Prevention Department of the Central Criminal Police Department (CPD).
53. To a large extent, the Cybercrime Prevention Department has taken over the function from the Economic Crime Directorate (ECED), which previously investigated cybercrime. Issues, typologies,

etc. described in the VCRA 2021. The information provided by the ECED remains valid.<sup>25</sup>

54. In addition, the CPD has pointed out that virtual assets still have the potential to be widely used to launder the proceeds of crime. As virtual assets and its service providers can be used at all ML stages, the predicate offences are manifold.
55. The cases of "money mules" are still topical - the CPD has a criminal case on file which reveals that members of an organised group carried out ML over a long period of time, using nearly 100 accounts opened with Latvian credit institutions. In these cases, the fraud proceeds were transferred into *Fiat* currency, which was then withdrawn in cash and converted into virtual currency. This has also led to the identification of unregistered virtual currency exchange service providers, which are not monitored and do not carry out customer due diligence, but do provide a *fiat* currency and virtual currency exchange service.
56. There are no cases of extortion and blackmail via email, where funds are requested to be transferred using virtual assets, in the CPD's case file.
57. From 2020 till August 2022, information was received on no less than 360 criminal proceedings initiated in the regional units of the SP in connection with illegal activities of bogus brokers, the coordination, cross-analysis and merging of which is carried out by the CPD. This criminal phenomenon has become a persistent international fraud trend, which is also developing and regularly targets Latvian nationals by involving them in high-risk transactions with virtual assets.
58. As part of an investigation launched in Latvia in March 2022, a major international operation, including with the support of the FIU, disrupted the operations of investment fraud call centres - two in Latvia and one in Lithuania. In total, at least 80 related parties were investigated and identified in Latvia. Preliminary estimates show that fraudsters made illegal profits of up to €3 million every month, mostly in virtual currency.
59. Between 1 January 2021 and August 2022, two criminal proceedings were initiated by the SP in connection with the encryption and ransom demand of Automated Data Processing System (ADAS) data. The offence is regularly reported, but investigations are largely not launched because the harmful consequences are not identified at the outset in such a way as to trigger criminal liability.
60. The SP welcomes the changes in the legislation on handling virtual asset in criminal proceedings, which is the result of the successful cooperation with the National Collateral Agency, which is responsible for the creation of wallets for storing virtual currency and the disposal of seized virtual currency. In accordance with subparagraph 76.2 of Cabinet Regulation of 27 December 2011 No 1025 "Regulations on the Disposal of Evidence and Seized Property", in order to ensure the sale of virtual currency, the NCA shall maintain a cryptocurrency wallet established for this purpose in Latvia or on the platform of a VASP registered in a Member State of the European Union, the European Economic Area or the North Atlantic Treaty Organisation.
61. When setting up a virtual wallet, the NCA assesses whether the service provider's platform is capable of making payments in the Single Euro Payments Area, whether the service provider is established in a country with which criminal justice cooperation can be ensured, and the type of virtual asset that can be used. According to the decision of the prosecutor in the criminal proceedings, on 16 June 2022, the sale of virtual currency took place, where virtual currency was sold for a total of EUR 328 000.
62. The CPD cites the following as obstacles to the investigation:
  - 62.1. lack of specific knowledge and practical reference material on handling virtual assets to enable all levels of investigative authorities to take the necessary steps to withdraw and transfer virtual asset to a cryptocurrency wallet in the possession of the NCA, and a common understanding of the procedural design of these steps;
  - 62.2. the relevant software to analyse virtual asset transactions is not currently available to the investigative authorities;
  - 62.3. the different perceptions of VASPs regarding cooperation with law enforcement authorities (these service providers often do not have a registered office and are therefore not linked to the jurisdiction of a particular country, thus making it impossible to implement the requirements of Part C of the Criminal Procedure Law on International Cooperation in Criminal Matters, and some service providers do not respond to calls for cooperation with law enforcement authorities,

<sup>25</sup> See VCRA 2021. Available:

<https://fid.gov.lv/uploads/files/2021/virtu%C4%81l%C4%81s%20val%C5%ABtas/VIRTUAL%20CURRENCIES.pdf>

- 
- ignoring such requests);
- 62.4. the execution of an arrest upon virtual asset stored on an online platform (e.g., Coinbase, Kraken, etc.) depends on that particular service provider, so there is a risk that the decision will not be enforced.
63. Bitcoin (BTC) and Ether (ETH) remain the most popular virtual currencies in the criminal world. Given the volatility of BTC and ETH, stablecoins are also used in the criminal environment, where the exchange rate is pegged to the USD or EUR, the most popular stablecoin being TETHER<sup>26</sup> (USDT), which runs on the Ethereum and TRON<sup>27</sup> blockchains. In recent years, it has been observed that stable currencies are used not only for transactions, but also for storing funds.
64. The information provided by the SRS TCPD also confirms that the situation described in the VCRA 2021 is still relevant:
- 64.1. Predicate offences in the SRS TCPD's case files/former criminal proceedings relate to tax evasion and fraud;
- 64.2. In the criminal proceedings of the SRS TCPD, almost all narcotic drugs or psychotropic substances ordered by mail (so-called "mail cases" initiated under Article 190.1(1) of the Criminal Law) are ordered via *DARKNET (TOR browser)*. Cryptocurrency is used to pay for narcotics. When requesting suspects' bank accounts, cryptocurrency purchases are frequently found (these purchases are qualified as circumstantial evidence in criminal proceedings, indicating that the person may be directly involved in ordering narcotic or psychotropic substances from DARKNET), but the SRS TCPD has no evidence (except when a person voluntarily presents his/her cryptocurrency wallet) that narcotic substances are being purchased using this particular cryptocurrency.
65. Similarly to the SP, the SRS TCPD also mentions the lack of technical means, appropriate IT solutions and professional analytical software as well as information exchange mechanisms capable of ensuring information exchange with other national authorities and VASPs as obstacles to the investigation.
66. The SRS TCPD also increasingly observes that current accounts are being opened on various foreign payment system platforms and, in order to conceal further cash flow, the criminally obtained funds are fully or partially converted into virtual assets to make it as difficult as possible to trace the funds.

<sup>26</sup> Tether - an asset-backed cryptocurrency stablecoin. Founded by Tether Limited Inc

<sup>27</sup> TRON - a decentralised, open-source blockchain-based operating system with smart contract functionality

## V. CONCLUSIONS

67. Considering that the regulatory framework in the AML/CFT Law and on licensing in the sector of virtual assets in Latvia has not changed in the last year and that VASPs identify the same problems. The opportunities for improvement of the regulatory framework mentioned in the VCRA 2021<sup>28</sup> have not lost their relevance and should be considered in the development of the regulatory framework planned by the MoF by 1 July 2023.
68. The number of VASPs is significantly higher both in Estonia, which has had a licensing mechanism for VASPs in place since 2017, and in Lithuania, which has a similar registration process for VASPs to the one in Latvia. This shows that not only is there a regulatory constraint on the development of the virtual asset sector in Latvia (lack of regulation), but also other conditions hinder its expansion (e.g., credit institutions' reluctance to open current accounts for VASPs).
69. There is a need to further develop a common understanding of the technology and nature of virtual assets in both the public and private sectors (VASPs, legislator, supervisory and control authority, financial sector, etc.).
70. The risks of ML/TF/PF have not changed significantly over the past year. NFTs and DeFi are playing an increasingly important role in the use of virtual assets for ML. The use of virtual assets or VASPs to circumvent sanctions and commit violations is possible, but is not seen as distinctly different from the use of other financial products and financial service providers.
71. The typologies and trends of suspicious transaction reports received by the FIU related to virtual assets remain the same, with credit institutions mainly reporting their customers as victims of cryptocurrency fraud.
72. In the cases under investigation involving virtual assets, the cases of "money mules", fake brokers and drugs purchased on DARKNET are still relevant and are the main ones. The main problems cited by law enforcement authorities are:
  - 72.1. lack of technical resources, adequate IT solutions and professional analytical software,
  - 72.2. the lack of, or differing perceptions of, information exchange mechanisms capable of sharing information with authorities and VASPs in other countries.

<sup>28</sup> VCRA 2021, p.5, paragraph 17. Available: <https://fid.gov.lv/uploads/files/2021/virtu%C4%81l%C4%81s%20val%C5%ABtas/VIRTUAL%20CURRENCIES.pdf>

## ABBREVIATIONS AND TERMS

<b>EU</b>	European Union
<b>FATF</b>	Financial Action Task Force
<b><i>Fiat</i> currency</b>	National coins and banknotes identified as legal means of payment and electronic money accepted as means of exchange in the country of issue
<b>FIU</b>	Financial Intelligence Unit
<b>FCMC</b>	Financial and Capital Markets Commission
<b>MoF</b>	Ministry of Finance
<b>MiCA</b>	EU single framework for virtual assets ( <i>Markets in Crypto-Assets</i> )
<b>MK</b>	Cabinet of Ministers
<b>ML</b>	Money laundering
<b>AML/CFT Law</b>	Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing
<b>NCA</b>	National Collateral Agency
<b>Action plan</b>	Cabinet Order No 122 of 22 February 2022 "On the 2022 Action Plan to Prevent Money Laundering, Terrorism and Proliferation Financing"
<b>PF</b>	Proliferation financing
<b>Risk Assessment</b>	Virtual Assets: Money Laundering and Terrorism and Proliferation Financing Risk Assessment
<b>TF</b>	Terrorist financing
<b>SRS</b>	State Revenue Service
<b>SRS TCPD</b>	Tax and Customs Police Department of the State Revenue Service
<b>SP</b>	State Police
<b>VCRA 2021</b>	The FIU's 2021 assessment of the risks of money laundering and terrorist and proliferation financing in virtual currencies
<b>VASP</b>	Virtual Asset Service Provider
<b>CPD</b>	Cybercrime Prevention Department of the Central Criminal Police Department of the State Police
<b>ECED</b>	Economic Crime Enforcement Department of the Central Criminal Police Department of the State Police