A Survey of Service Providers of Virtual Currency

Financial Intelligence Unit, September 22, 2020

A Short Summary

In the survey compiled by the Estonian Finance Intelligence Unit (*henceforth RAB*), a review is given of virtual currencies (*henceforth VC*), of services and the market participants connected to virtual currencies. There is also an analysis of the risks of virtual currencies connected to money laundering and terrorist financing. The survey puts forward the schemes and practices of unlawful use of virtual currencies. The immediate cause of the survey is that the rapid growth in the use of virtual currencies and the number of service providers in the past years has also enhanced the risks of criminality in the field. The information that has reached the *RAB* as well as the information that has been gathered for the survey indicate that virtual currencies are exploited also in Estonia for hiding criminal income and for money laundering as well as for committing fraud and for buying illegal goods and services.

In the years 2018–2019, the number of service providers in the field of VC that have applied for an operating licence [in Estonia], has grown very rapidly (in the years 2017–2019 operating licences in the field of VC were issued to more than 1300 enterprises), because Estonia was one of the first countries where an obligation of an operating licence in VC was introduced. The analysis of the *RAB* indicates that **enterprises that have an operating licence in VC are very often connected to Estonia only by the fact that they are registered here. The actual business activities, the board of directors, beneficiaries and also customers are situated abroad** - facts that make it difficult to conduct supervision and to handle cases with elements of criminal offence; at the same time, the great number of enterprises with an operating licence causes a great risk of reputation loss for Estonia. In addition to that, the analysis of the *RAB* revealed that the due diligence measures of enterprises with an operating licence in VC are clearly inadequate. The given problem was to a certain extent addressed by an amendment to the Money Laundering and Terrorist Financing Prevention Act (*henceforth RahaPTS*) that entered into force in March 2020, according to which the enterprises with an operating licence in VC must have a business establishment in Estonia. Despite that, it is likely that the level of diligence of the enterprises of the sector does not take a great leap forward, a reason why the sector of VC should receive continuously extra attention in the field of the processes of issuing operating licences and conducting supervision as well as from the investigation institutions. On the basis of the results of the survey, the *RAB* is of the opinion that the rules of the regulation concerning virtual currencies should be made more strict and that for the service providers of VC a reporting obligation should be introduced, comparable to that of financial institutions, concerning the transactions, customers and the amount of mediated transactions.

Methodology

As sources of data, the survey has used the results of the questionnaire of an inquiry conducted among service providers of virtual currency, websites of service providers, data of the [Estonian] Commercial Register and the Register of Economic Activities as well as interviews with specialists of [the Estonian] Police and Border Guard Board.

The translator Kristi Ugam is aware of the requirements of the [Estonian] Code of Criminal Procedure (*KrMS*) § 161 and of the responsibility laid down in § 321 of the [Estonian] Penal Code (*KarS*) (signed digitally).

Enterprises that have been granted and operating licence in Estonia to provide a service of VC are defined in the survey as providers of a service of virtual currency in Estonia.

At the end of the year 2019, the Financial Intelligence Unit instituted an inquiry among all the entrepreneurs to whom, according to the Register of Economic Activities, an operating licence for offering a service of exchanging VC for money and/or for providing custodian wallets was issued before June 30, 2019. Those entrepreneurs to whom a valid operating licence was issued before June 30, 2019 for offering both of the VC services, had to fill in the inquiry questionnaires of both sectors, because the questions concerning exchanging VC for money and the questions for the virtual currency wallet providers were somewhat different. In total, the questionnaire of the inquiry was sent out to be answered by 855 enterprises: 846 providers of the service of exchanging VC for money and 750 virtual currency wallet providers.

As a result of the instituted inquiry, the questionnaire of the inquiry was filled in by 448 providers of the service of exchanding VC for money and by 391 virtual currency wallet providers. According to what was put down in the questionnaire, 262 enterprises that had answered the questionnaire had started providing the service of exchanging VC for money in Estonia, having a valid operating licence for exchanging VC for money, and 212 enterprises that had answered the questionnaire had started providing the service, having a valid licence to provide the virtual currency wallet. There were 280 unique enterprises among them.

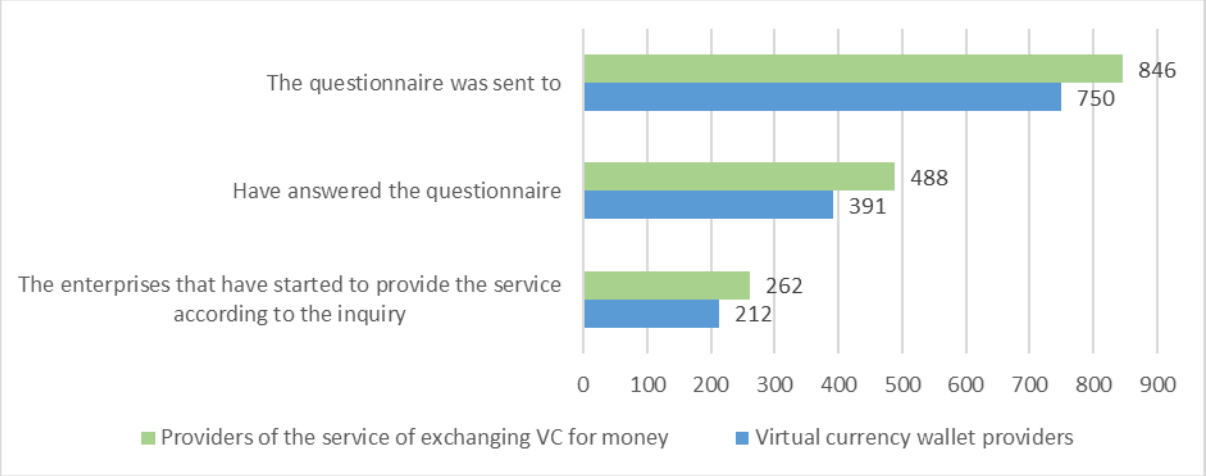

Diagram 1. An overview of the enterprises that received and answered the inquiry questionnaire of the *RAB* and that have started business activities.

In order to give an overview of the sector, the data of the Commercial Register and of the Register of Economic Activities (*MTR*) were used for the current survey. Also, the websites of all the VC service providers who had answered the questionnaire and had started to provide the service, were analysed in order to map the character of the activity of the VC service providers and to define exactly which services are provided.

In case of the 43 enterprises that have the largest turnover from mediating services, a thorough background analysis was made in order to determine the activity profile (for whom are the services meant, which countries have the priority in providing the service *etc.*). In the focus of the analysis there were those enterprises, the turnover of whose mediated transactions was, according to the data of the

inquiry, more than a million euros in the year 2018 or in the first half of the year 2019. For the background analysis, in addition to the public information sources also the data of the Commercial Register were used. Also, a Commercial Register excerpt was taken about the associated persons, the addresses and the activities of the VC service providers that have an Estonian operating licence. The possible origin of the natural persons associated with the service providers was analysed and the personal codes were also connected to the database of the e-residents.

In the framework of the inquiry, also two interviews were made with representatives of the Estonian Police and Border Guard Board. In the interviews, the central question was how virtual currecies are taken advantage of in criminal schemes, money laundering included. In addition to that, officials of the supervisory service of the *RAB* were interviewed about the issues concerning the supervision of the VC service and the issues concerning operating licences, as well as officials of the Estonian Internat Security Service concerning risks that are caused by financing of terrorism.

The translator Kristi Ugam is aware of the requirements of the [Estonian] Code of Criminal Procedure (*KrMS*) § 161 and of the responsibility laid down in § 321 of the [Estonian] Penal Code (*KarS*) (signed digitally).

1 A short Introduction into Virtual Currencies

There are more than 2000 different virtual currencies in circulation in the world[1]. Most of the virtual currencies use blockchain technology. The blockchain that is the foundation of the virtual currrencies, constitutes a divided digital database that saves transactions and that cannot be changed, making the data non-falsifiable and durable. The details of transactions are public and utterly observable[2].

Virtual currencies are dividend into centralized and decentralized virtual currencies. The centralized virtual currencies have a central administrator, who launches virtual currencies, administers the use of them and removes them from the circulation. They can often be found in internet environments that offer alternative payment networks or online-games. The decentralized virtual currencies, for example Bitcoin, do not have such a central administrator.[3]

In a narrower sense, it is possible to specify crypto-currency under virtual currencies. This is a monetary system that has been built up on cryptographical bases and is usually decentralized and self-regulating. For a user, crypto-currency is rather transparent, because transactions are publicly observable; on the other hand, it affords anonymity. Most of the best-known virtual currencies, as Bitcoin, Ethereum, classify into the category of cryptocurrency[4].

Also the so-called stablecoins, the price of which is connected to the value of certain concrete assets, most usually 1:1 US dollar (e.g. Tether, USA Coin, Paxos), fall into the category of virtual currencies. In addition to that, a stable coin Libra that combines several currencies, is currently being developed; that works as a digital composite Libra, consisting of stable coins of a single currency (USD, EUR, GBP). Even though stable coins in essence do not generate any higher risks than virtual currencies in general do, their greater potential to be massively taken into use has made political decision-makers cautious, as the consequenties cannot be precisely estimated[5].

In the fifth Directive on the prevention of financing of money laudering and terrorism[6] (*henceforth Directive (EU) 2015/849*) article 1 (2) d), VC is defined as follows:

> *"Virtual currencies" 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*

[1] Haffke, L., Fromberger, M., Zimmermann, P. (2019). *Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and How to Address Them*. Journal of Banking Regulation, Forthcoming. https://ssrn.com/abstract=3328064
[2] Ärileht. Plokiahela tehnoloogia. 14.01.2019
[3] Keatinge, T., Carlisle, D., Keen, F. (2018). *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*. European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs.
[4] https://www.kryptoraha.ee/tehnoloogia/
[5] FATF. (2020). Virtual Assets – Draft FATF Report to G20 on so-called Stablecoins
[6] 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. Official Journal of the European Union, June 19, 2018, L156/43-74. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1602693516196&uri=CELEX:32018L0843.

The translator Kristi Ugam is aware of the requirements of the [Estonian] Code of Criminal Procedure (*KrMS*) § 161 and of the responsibility laid down in § 321 of the [Estonian] Penal Code (*KarS*) (signed digitally).

or legal persons as a means of exchange and which can be transferred, stored and traded electronically.

In the Directive (EU) 2015/849, it is pointed out that virtual currencies should be mixed up neither with electronic money[7] nor with monetary means in the broader sense[8] nor with local payment instruments of member states nor with a gaming currency, which can only be used in a concrete gaming environment.

To rephrase the definitions of the Directive (EU) 2015/849 and The [Estonian] Money Laundering and Terrorist Financing Prevention Act[9] in a slightly less complicated way, VC means a value represented in the digital form, which is digitally transferable, preservable or tradable, which is indeed not a legal payment nor monetary instrument under any jurisdiction, but which is used by natural or legal persons as a payment instrument.

In Estonia, virtual currencies are defined in the sense of The Income Tax Act § 15 subsection 1 as property and tax is charged on the gains from them (gains from the sale, from wages, from business profits gained from mining) according to similar principles to taxing gains that have been earned in a traditional currency[10].

1.1 The regulation of the service of virtual currency in Estonia

Providers of a VC service[11] are obliged subjects to The [Estonian] Money Laundering and Terrorist Financing Prevention Act, in other words, they must obey the rules of the Act; in order to offer a VC service, entrepreneurs have to apply for a relevant operating licence from the *RAB* and their activities are subject to the supervision of the *RAB*. According to the information that the *RAB* has received, there have been several occasions of trying to offer VC services in Estonia without an operating licence; that information has been confirmed by misdemeanour procedures that have been conducted by the *RAB*.

---

[7] Defined in the Directive 2009/110/EC of the European Parliament and the Council (1) Article 2 point 2 as electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt fo funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer.

[8] According to the Directive 2015/2366 of the European Parliament and of the Council (2) Article 4 point 25, it [´funds´] means banknotes and coins, scriptural money and electronic money.

[9] The Money Laundering and Terrorist Financing Prevention Act § 3 p 9: *´Virtual currency´ means a value represented in the digital form, which is digitally transferable, preservable or tradable and whcih natural persons or legal persons accept as a payment instrument, but that is not the legal tender of any country or funds for the purposes of Article 4 (25) of Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market, amending Directives 2002/65/EÜ, 2009/110/EÜ and 2013/36/EL and Regulation (EL) nr 1093/2010 and repealing Directive 2007/64/EÜ (ELT L 337, 23.12.2015, lk 35–127) or a payment instrument or a payment transaction for the purposes of points (k) and (l) of Article 3 of the same Directive.*

[10] https://www.emta.ee/et/eraklient/tulu-deklareerimine/muu-tulu/eraisiku-virtuaalses-valuutaskruptovaluutas-saadud-tulu

[11] A virtual currency service means a wallet service in the framework of which keys are generated for customers or customers´ encrypted keys are kept, which can be used for the purpose of keeping, storing and transferring virtual currencies, as well as a virtual currency exchange service with the help of which a person exchanges a virtual currency against money or money against a virtual currency or a virtual currency against another virtual currency (The [Estonian] Money Laundering and Terrorist Financing Prevention Act § 3 subs. 9^1, 10, 10^1).

The translator Kristi Ugam is aware of the requirements of the [Estonian] Code of Criminal Procedure (*KrMS*) § 161 and of the responsibility laid down in § 321 of the [Estonian] Penal Code (*KarS*) (signed digitally).

Estonia is one of the first countries in the world where one started to regulate the activities of providers of VC services. In the course of time significant changes have taken place in the regulations. In connection to providers of a service of a virtual currency a higher risk of money laundering was seen in Estonia in 2006 already, when it was discovered that the developments in information technology enable new opportunities for money laudering practices that cannot be controlled by regulations. That is why the so-called providers of nontraditional means of payment were subjected to the regulation of The [Estonian] Money Laundering and Terrorist Financing Prevention Act that came into force in 2008, under the term provider of service of alternative means of payment.

In the § 6 (2) 4) of the version of The Money Laundering and Terrorist Financing Prevention Act that was then in force[12], a provider of a service of alternative means of payment was defined as a person who, in the framework of his/her economic or professional activities, buys, sells or mediates, through a system of communication, transmission or clearing, funds that have a monetary value, that offer a possibility to cover monetary duties or that can be exchanged for a valid currency, but who is neither a credit institution nor a financial institution in the sense of the Credit Institutions Act. The relevant service providers were subjected to the obligation that applies to financial institutions, to apply due diligence measures, as well as the obligation to sign up in the Register of Economic Activities.

The [Estonian] Supreme Court has sentenced in 2016 that trading in crypto-money, included Bitcoins, as an economic activity corresponds to the term of providing a service of instruments of alternative payment, and that, as such, it is subject to the regulation of money laundering prevention and to the governement supervision. In addition to that, the Supreme Court was of the opinion that the location of the server of the service provider and processing transactions at least partly in servers abroad neither prohibits the application of The Money Laundering and Terrorist Financing Prevention Act nor is the only relevant condition for determining the jurisdiction.[13]

In the new Money Laundering and Terrorist Financing Prevention Act that came into force in 2017[14], the term of a provider of a service of alternative means of payment was substituted for two groups of VC service providers: providers of a service of exchanging a virtual currecy for a fiat currency and a virtual currency wallet service providers[15]. Doing that, Estonia became the first country in the EU that started to follow the provisions of the Directive (EU) 2018/843 that apply to virtual currencies[16]. The change has a serious seamy side though, that made the business in the sector practically uncontrollable: the restrictions that applied before, were abolished, and the threshold for the obligation of due diligence was lifted to 15 thousand euros.

The first operating licences for offering a VC service were issued in Estonia in the late autumn of 2017 when the new Money Laundering and Terrorist Financing Prevention Act came into force. While the numbers of operating licences issued were modest in the first year – respectively four licences for

[12] The [Estonian] Government Gazette I 2008, 3, 21.
[13] The Resolution No 3-3-1-75-15 of the Administrative Law Chamber of the Supreme Court of April 11, 2016.
[14] The [Estonian] Government Gazette I, 17.11.2017, 2
[15] According to the definition of the Directive (EU) 2018/843 Article 1(2)(19), a virtual currency wallet service provider [custodian wallet provider] means an entity/a person that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies. The Money Laundering and Terrorist Financing Prevention Act that is currently in force, § 3 p 10 defines a virtual currency wallet service as a service in the framework of which keys are kept, which can be used for the purpose of keeping, storing and transferring virtual currencies.
[16] https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/estonia

exchanging a virtual currency for a fiat currency/for money and two licences for the wallet service –, that was followed by an explosive rise in applications for operating licences. In the year 2018, already 612 operating licences were issued for exchanging a virtual currency for money and 525 operating licences for provinding the wallet service; in 2019 the figures were 666 and 638 respectively.

The rapid rise in the number of operating licences was a telling sign about the shortcomings of the regulation then: the *RAB* did not have a legal basis for denying issuing a licence, even to an enterprise that did not have any actual connection to Estonia (*further chapter 2.4*). That caused a significant risk of reputation loss for Estonia, as many enterprises were connected to organizing fraude and affording money laundering, whereas it was essentially impossible to supervise enterprises that are operational abroad, among other things to apply control locally.

At the end of 2019, Riigikogu, the Estonian Parliament, introduced significant amendments in the regulation of virtual currencies in The Money Laundering and Terrorist Financing Prevention Act[17], which tightened the standards of providing a VC service: a prerequisite for possessing a VC operating licence is that the seat of the entrepreneur (the headquarters) is situated in Estonia and that there is thus a significantly tighter connection to Estonia. Additionally, the enterprises must be established in Estonia or must operate here through a subsidiary company. That makes it possible to conduct supervision significantly more efficiently. As a result of the amendments in the law, the same rules that had been previously applied on the basis of the Money Laundering and Terrorist Financing Prevention Act on financial institutions, started to be applied to providers of VC services. On the list of services that require an operating licence, the service of exchanging a virtual currency for a virtual currency was added. Previously, such an activity was not regulated and the requirements of The Money Laundering and Terrorist Financing Prevention Act were not obligatory - facts that caused that the *RAB* did not have an overview of the number of service providers and the scope of the activity in Estonia and did not have an opportunity to conduct supervision. With the amendment of the end of 2019 the previously differentiated notions of VC services were united under the umbrella term virtual currency service[18] (MLTFPA § 2 subs. 2).

The equalisation with financial institutions meant for VC service providers more severe requirements for applying due diligence measures. Whereas previously a VC service provider was not obliged to identify a customer when it concerned some occasional transactions in the value of less than 15,000.00 EUR, now the customer identity check and verification of data do not depend on the value of a translaction any more, the person concerned must be identified in any case. Also, the rules for the identity check of citizens of the third countries became more strict. The amendments of the law came into force on March 10, 2020. The enterprises that already possessed a VC operating licence were subjected to the obligation to adapt their activity to the amendments at the latest by July 1, 2020.

The amendments brought rapidly significant results. Primarily, the problem that VC enterprises are active abroad and are only formally connected to Estonia was alleviated. Since March 2020, the *RAB* had become able to conduct supervision much more efficiently, to react more efficiently on violations of the

[17] RT I, 31.12.2019, 2

[18] In the analysis conducted in the framework of the present survey, the services of exchanging a virtual currency for money and providing a virtual currency wallet are often still differentiated, as in the data of the Register of Economic Activity the services of exchanging a virtual currency for money and providing a virtual wallet are differentiated, as well as in the answers to the questionnaire of the inquiry conducted among the service providers.

rules and to apply coarcive measures. The *RAB* has systematically reduced the number of enterprises whose business activities are actually not connected to Estonia or who failed to observe precepts (earlier, the *RAB* had also difficulties for example to receive answers to information requests). With the help of the amendment, significantly less new VC operating licences have been issued: on the one hand, the number of applications for a licence has reduced in the framework of more severe requirements, and on the other hand, the *RAB* has applied the requirement of an irreproachable business reputation in the processing of the licence applications. The latter enables it to refuse issuing an operating licence to entrepreneurs with a suspicious background. During the period of March 1, 2020 – July 31, 2020, the *RUB* declared in total 1296 licences null and void, concerning 705 different enterprises. Hence, the attractiveness of the jurisdiction here has considerably declined for VC service providers who are not operational in Estonia, but, all things considered, that is a positive shift as it has not influenced the tax revenue and enterprises that are actually active in Estonia, get a certain competitive advantage.

2 Providers of a virtual currency service in Estonia

Since the end of the year 2017, the number of VC service providers grew very rapidly in Estonia: the Financial Intelligence Unit issued in the years 2017-2019 in total 1282 operating licences for exchanging virtual currency for money and 1165 operating licences for providing a vitual currency wallet. There were in total 1308 unique enterprises with one or several VC operating licences.

Table 1. The number of operating licences issued by the Financial Intelligence Unit in 2017–2019.

	2017	2018	2019	IN TOTAL
Exchange for VC service	4	612	666	1282
Virtual currency wallet service	2	525	638	1165
Unique enterprises	4	617	687	1308

Source: Register of Economic Activities

While at the end of March 2020 there were 869 enterprises that had an operating licence issued in Estonia for providing a virtual currency wallet and 946 enterprises that had a valid operating licence for exchanding virtual currency for money[19], the market could considerably be ordered by the amendment of the Money Laundering and Terrorist Financing Prevention Act that came into force on March 10, 2020 and that was mentioned in the previous chapter. In March 2020, 340 operating licences were withdrawn, in April the indicator was 194, in May 73, in June 47 and in July even 644, primarily due to the fact that enterprises with a valid operating licence had to adapt themselves at the latest by July 1, 2020 to the requirements that had entered into force on March 10, 2020 but did not do that. In addition to that, 529 owners of different operating licences have temporarily terminated their activity, in total 285 different enterprises. That means that, with the stand of August 1, there were in total 611 various VC operating licences (295 licences for exchanging VC for money, 261 for the wallet service and 55 for VC service), that is compared to the stand of the end of March approximately three times less. The correspondence to the requirements of the amendment that came into force in March of a great part of those enterprises is still being checked, due to which the number of enterprises that have the operating licence in Estonia may still decline.

[19] An operating licence for providing both services of virtual currencies was in possession of 849 enterprises, 20 enterprises had a licence to provide only a VC wallet and 97 enterprises to offer the service of exchanging VC for money.

The translator Kristi Ugam is aware of the requirements of the [Estonian] Code of Criminal Procedure (*KrMS*) § 161 and of the responsibility laid down in § 321 of the [Estonian] Penal Code (*KarS*) (signed digitally).

Table 2. The number of valid VC operating licences 2017 – August 2020.

	2017	2018	2019	08.2020
The service of exchanding VC for money	4	595	1210	296
VC wallet service	2	512	1104	261
VC service	-	-	-	55
Unique enterprises	4	599	1234	353

Source: Register of Economic Activities

On the basis of the new regulation that came into force in March, 13 operating licences for providing a service of virtual currencies have been issued, 29 in May, 23 in June, and 9 in July.

2.1 Providers of a virtual currency service until spring 2020

The enterprises that had an operating licence in Estonia in March 2020 were young, in majority established either in 2018 or in 2019 (respectively 47% and 41%). 96% of the enterprises were not established before 2016.

In the Commercial Register, the enterprises that offer VC services have registered themselves under a broad scale of industries; in total, there are 82 different industries mentioned. Preponderantly the most, 40% of the VC service providers, have mentioned "Other financial service activities, except insurance and pension funding" as their industry; widespread is also "Business support service activities n.e.c." (13% of the enterprises that offer a VC service) and "Computer programming activities" (10% of the enterprises).

As a part of the survey, an analysis of the websites of the providers of VC services was conducted, in the framework of which the websites of all the enterprises that had answered the questionnaries and had started their business were studied. It turned out that while the main industry of the majority of the enterprises that possess an operating licence of VC is trading in virtual currencies or offering a wallet service, many enterprises are such that only rely on virtual currencies, offering a different service. For example, there are financing platforms, live streaming platforms, investment and cowdfunding platforms among them, but also enterprises that offer loans that use crypto-currency as collateral. Among service providers, there are also those who issue tokens themselves and those that organise Initial Coin Offering i.e. ICO for other enterprises, that is comparable to stock market launch / initial public offering (IPO).

In the framework of the inquiry in the VC service providers that was conducted before the convergence of the terminology of VC services, it was discovered, equally to the findings of the analysis of the opering licences, that most of the enterprises offer the service of exchanging VC for money as well as the wallet service. At the end of the year 2019, 280 enterprises among the addressees of the inquiry questionnaire were operational in Estonia in the VC sector (i.e. had started providing a VC service); 193 of them had started providing both services, 69 only exchanging VC for money and 18 providing a VC wallet.

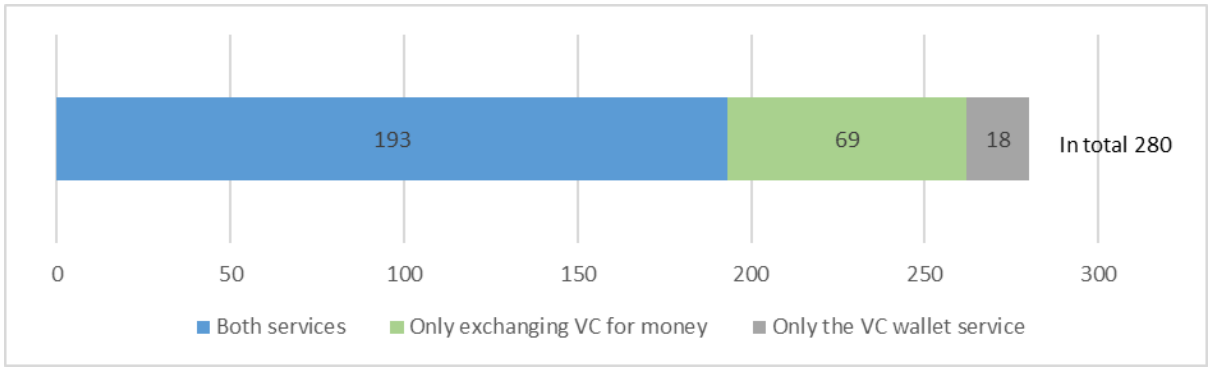

Diagram 2. The division of enterprises that have answered the questionnaire according to the VC service.

2.2 The turnover of transactions and clientèle of the service providers

The results of the inquiry show that the total turnover of the services that were mediated by enterprises that are active on the Estonian market providing services of virtual currency has increased rapidly. While in 2018 the calibre of that was 590 million euros, in the first half of 2019 it was twice as high already – 1,2 billion euros. The turnovers of mediating VC services vary largely among enterprises. During both periods, the majority of the turnover belonged to one enterprise, respectively 420 million euros in 2018 and 820 million euros in the first half of 2019. Among the enterprises that had started their business activities, the median turnover of the mediated transactions was 94 thousand euros in 2018 and 50 thousand euros in the first half of 2019. 83, i.e. approximately one third of the VC enterprises, noted in their answers to the questionnaire that they had mediated services in 2018; concerning the first half of 2019, already 188 enterprises noted that.[20] A division of enterprises according to the turnover of the transactions mediated by the service providers is depicted on the diagram 3.

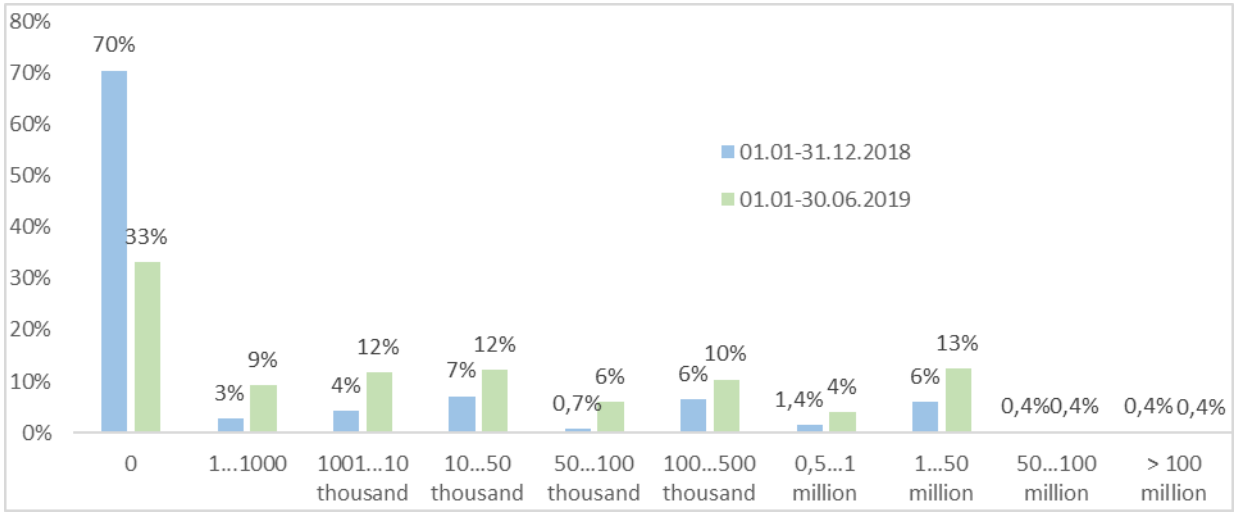

Diagram 3. A division of enterprises according to the turnover of the mediated transactions

[20] What makes pointing out the precise turnover number difficult, is the fact that many enterprises that have answered the questionnaire of the inquiry and that have started operating on the Estonian market providing the service of exchanging VC for money as well as providing a wallet, entered in both questionnaires the same turnover number. In the analysis, one of the double entries was removed.

Summarized information about the business relationships and the turnovers of the mediated transactions of the enterprises can be found in the table 3.

Table 3. The number of business relationships and the turnover of mediated translactions of the providers of virtual currency services that have started business activities in Estonia

	Indicator	During the period 01.01–31.12.2018	During the period 1.01.-30.06.2019
VC in total, n=280	The number of business relationships that have been entered into in order to provide a virtual currency service	278 thousand, including one enterprise that had 177 thousand	500 thousand, including one enterprise that had 180 thousand
	Companies whose indicator was > 0	*93 (34% of enterprises)*	*186 (67% of enterprises)*
	The total turnover of providing a virtual currecy service (EUR)	590 million, including one enterprise that had 420 million	1,2 billion, including one enterprise that had 820 million
	Enterprises whose indicator was > 0	*83 (30% of the enterprises)*	*187 (67% of the enterprises)*
VC for money, n=262	The number of business relationships that have been entered into in order to provide a virtual currency service	233 thousand, including one enterprise that had 177 thousand	285 thousand, including one enterprise that had 154 thousand
	Enterprises whose indicator was > 0	*78 (30% of the enterprises)*	*159 (61% of the enterprises)*
	The total turnover of providing a virtual currecy service (EUR)	178 million, including one enterprise that had 60 million	296 million, including one enterprise that had 80 million
	Enterprises whose indicator was > 0	*73 (28% of the enterprises)*	*169 (65% of the enterprises)*
VC wallet service, n=211	The number of business relationships that have been entered into in order to provide a virtual currency service	73 thousand	270 thousand, including one enterprise that had 150 thousand
	Ettevõtteid, kellel oli näitaja > 0	*62* (29% *of enterprises*)	*133* (63% *of enterprises*)
	The total turnover of providing a virtual currecy service (EUR)	440 million, including one enterprise that had 400 million	986 million, including one enterprise that had 800 million
	Enterprises whose indicator was > 0	*45* (21% *of the enterprises*)	*112 (53% of the enterprises)*

The source: The inquiry among the providers of a virtual curency service

The graphic division of the enterprises of the whole sector accoring to the business relationships that they have entered into in order to provide a virtual currency service, is depicted on the diagram 4.

The translator Kristi Ugam is aware of the requirements of the [Estonian] Code of Criminal Procedure (*KrMS*) § 161 and of the responsibility laid down in § 321 of the [Estonian] Penal Code (*KarS*) (signed digitally).

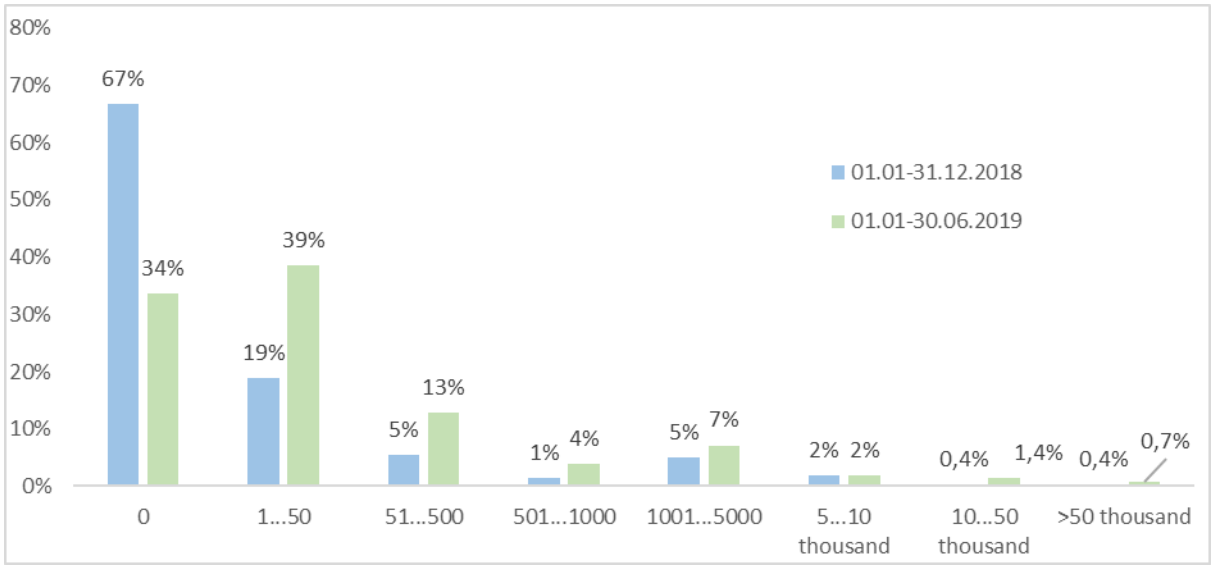

Diagram 4. The division of the enterprises accoring to the number of business relationships that they have entered into in order to provide a virtual currency service

The number of the business relationships that were entered into in order to provide a virtual currency service increased rapidly during the analysed period, similarly to the turnover of the mediation of the service. In 2018 it was 280 thousand, in the first half of 2019 500 thousand already. With that, the increase appears in each size category, that means that new enterprises have emerged in the category of a small, as well as a medium and a large number of business relationships.

The number the business relationships that have been entered into with persons of a government background has increased in an even more rapid tempo. In the first half of the year 2019, the indicator had more than doubled in comparison to 2018, respectively 376 and 162 business relationships that were entered into. A refusal to enter into a business relationship or a refusal of an occasional transaction occurred in the first half of 2019 in 60 thousand cases, whereas the suspicion of money laundering was the reason for terminating a business relationship only in 584 cases out of all business relationships entered into. It is also important to note that 39 enterprises that provide the service of exchanging a virtual currency for money, were ready to offer transactions without business relationships (since March 10, 2020 that practice does not comply with the law any more); in such a way, the service has been used by 36 000 customers. The enterprises specified one third of the customers of their services as customers of a higher risk.

91% of the enterprises that had started to provide a service of virtual currency in Estonia offered in the time of answering the questionnaire an opportunity to trade in or store Bitcoin. Widespead virtual currencies that are traded in, are aslo Ethereum (67%), Litecoin (44%) and Bitcoin Cash (44%). 8% of the enterprises accept cash while providing the service. The size of those enterprises can be estimated on the basis of the diagram 5 where the division has been depicted on the basis of the total turnover of the mediation of the service in the first half of the year 2019.

The translator Kristi Ugam is aware of the requirements of the [Estonian] Code of Criminal Procedure (*KrMS*) § 161 and of the responsibility laid down in § 321 of the [Estonian] Penal Code (*KarS*) (signed digitally).

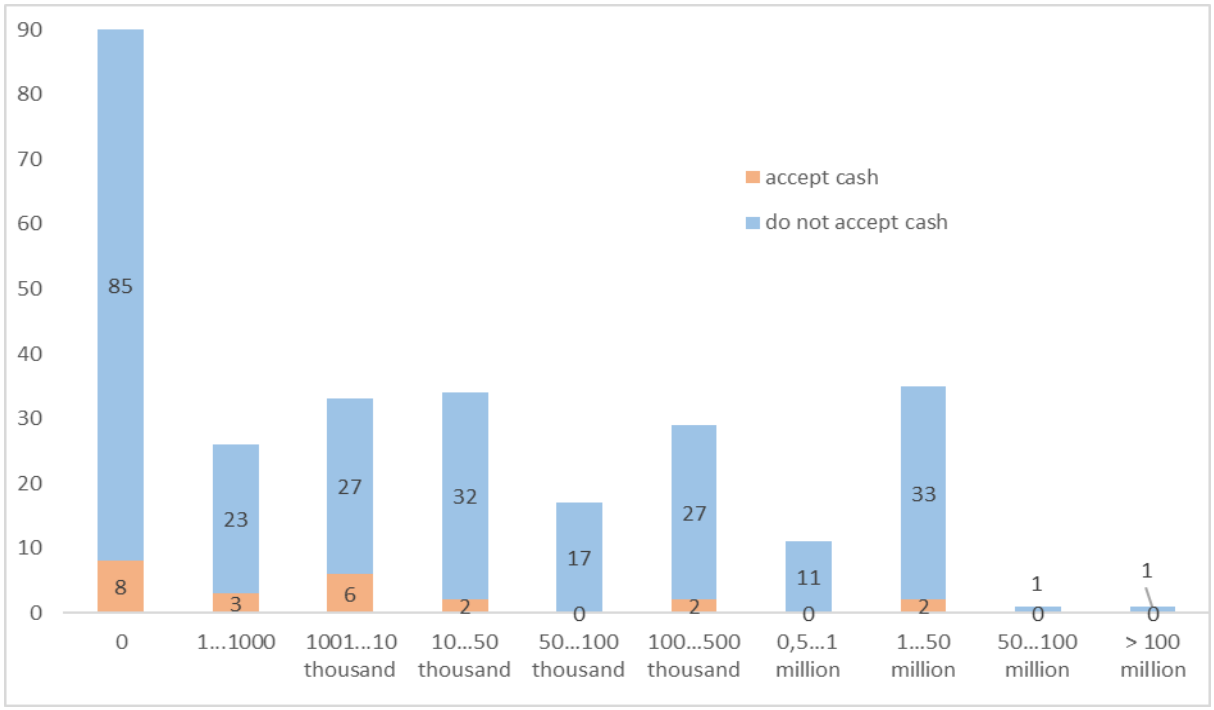

Diagram 5. The division of the enterprises that accept cash, on the basis of the total turnover of the mediation of the service in the first half of the year 2019

Among those enterprises that offered the service of exchanging VC for money, 84% exchanged the euro, 42% the US dollar and 13% the Russian rouble. The division of the given enterprises on the basis of the total turnover of the services mediated during the first half of the year 2019 is depicted on the diagram 6.

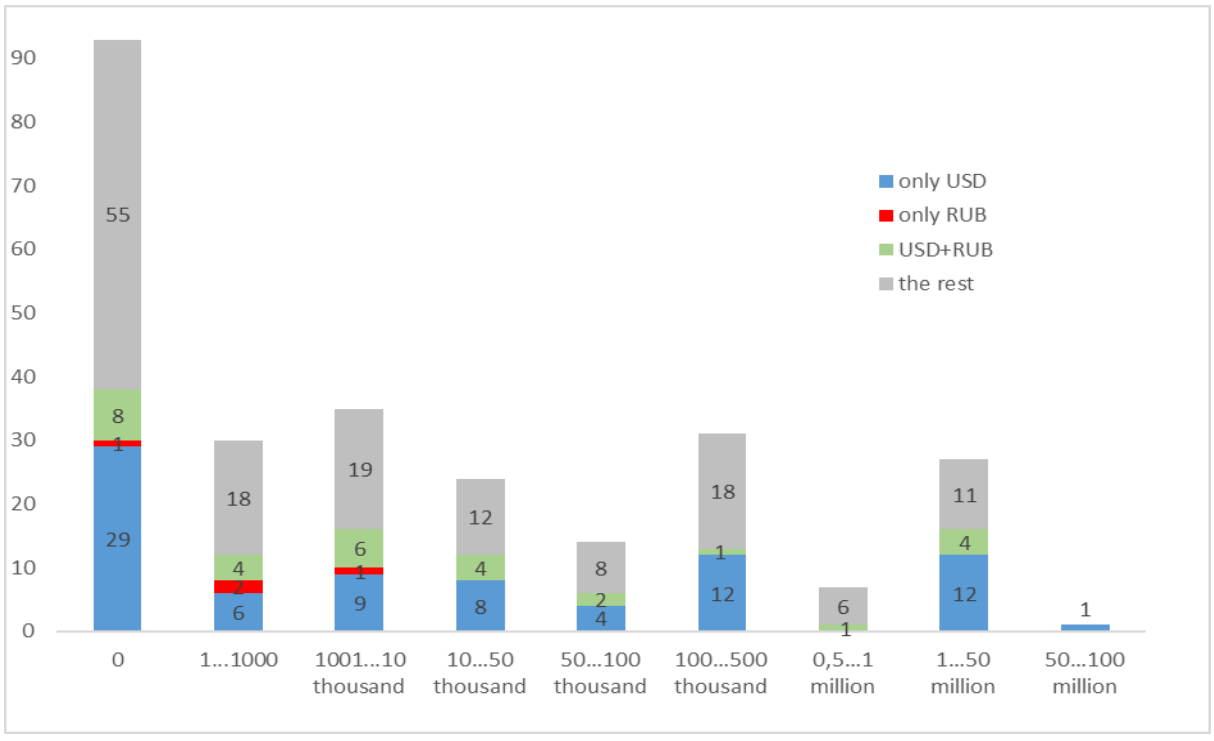

Diagram 6. The division of the enterprises that exchange the US dollar and the Russian rouble, on the basis of the turnovers of the first half of the year 2019 of the mediated services

The translator Kristi Ugam is aware of the requirements of the [Estonian] Code of Criminal Procedure (*KrMS*) § 161 and of the responsibility laid down in § 321 of the [Estonian] Penal Code (*KarS*) (signed digitally).

Among the enterprises that fall into the category "the rest" (in total 147), only 116 mediated euro according to the data of the questionnaire. 31 enterprises did not mediate any of the currencies that were mentioned in the menue of the questionnaire (EUR, USD, RUB); 26 of them do not exchange any currency and the remaining five noted the Polish zloty, the Japanese yen, the Vietnamese dong, the Venezuelan bolivar or the Singaporean dollar as an answer.

2.3 The due diligence measures

Although the total turnover of the services mediated, as noted in the questionnaire, does neither offer an opportunity to precisely estimate the size and growth of the Estonian market nor the scope and increase of transactions, it refers to the growing basis of virtual currencies and the activity of the market that the number of employees in Estonia of the VC enterprises, the task of whom it is to follow the rules imposed by the Money Laundering and Terrorist Financing Prevention Act, has increased in the first half of the year 2019 to 152 in comparison to the 102 reported in 2018. The number of the employees of the enterprises that have answered the questionnaire, and the number of employees in Estonia, has been presented in the table 4.

Tabel 4. The number of employees of the enterprises of virtual currency services that have srtarted business in Estonia

	Indicator	During the period 1.01.–31.12.2018	During the period 1.01.–30.06.2019
VC in total, n=280	The number of employees whose task it is to follow the rules imposed by the Money Laundering and Terrorist Financing Prevention Act while providing a service	426	620
	Enterprises whose indicator was > 0	*175 (63% of enterprises)*	*246 (88% of enterprises)*
	The number of employees in Estonia whose task it is to follow the rules imposed by the Money Laundering and Terrorist Financing Prevention Act while providing a service	102	152
	Enterprises whose indicator was > 0	*76 (27% of enterprises)*	*115 (41% of enterprises)*
VC for money, n=262	The number of employees whose task it is to follow the rules imposed by the Money Laundering and Terrorist Financing Prevention Act while providing a service	414	596
	Enterprises whose indicator was > 0	*164 (63% of enterprises)*	*231 (88% of enterprises)*
	The number of employees in Estonia whose task it is to follow the rules imposed by the Money Laundering and Terrorist Financing Prevention Act while providing a service	98	147
	Enterprises whose indicator was > 0	*72 (27% of enterprises)*	*110 (42% of enterprises)*
VC wallet service, n=211	The number of employees whose task it is to follow the rules imposed by the Money Laundering and Terrorist Financing Prevention Act while providing a service	326	462
	Enterprises whose indicator was > 0	*125 (59% of enterprises)*	*180 (85% of enterprises)*
	The number of employees in Estonia whose task it is to follow the rules imposed by the Money Laundering and Terrorist Financing Prevention Act while providing a service	75	111
	Enterprises whose indicator was > 0	*59 (28% of enterprises)*	*88 (42% of enterprises)*

The Source: The inquiry of the providers of a virtual currency service

The translator Kristi Ugam is aware of the requirements of the [Estonian] Code of Criminal Procedure (*KrMS*) § 161 and of the responsibility laid down in § 321 of the [Estonian] Penal Code (*KarS*) (signed digitally).

Application of due diligence measures varies greatly among the enterprises that answered the questionnaire. The majority of the enterprises claimed that they monitor the background of all their customers, but a monitoring depending on the risk profile of the business relationship is also common, or, to a smaller extent, depending on the limit of the transaction. More than half of the enterprises use external service providers to follow the principle "know your customer" (KYC). Less common, but still regular, is the use of external service providers to follow the principle of "know your transactions"; in general the service providers are the same as those who are used for KYC.[21]

In 2019, the number of reports that the *RAB* [Financial Intelligence Unit] received from the VC service providers increased sharply in comparison to the previous years. The change in time in the number of reports filed per semester has been presented on diagram 7.

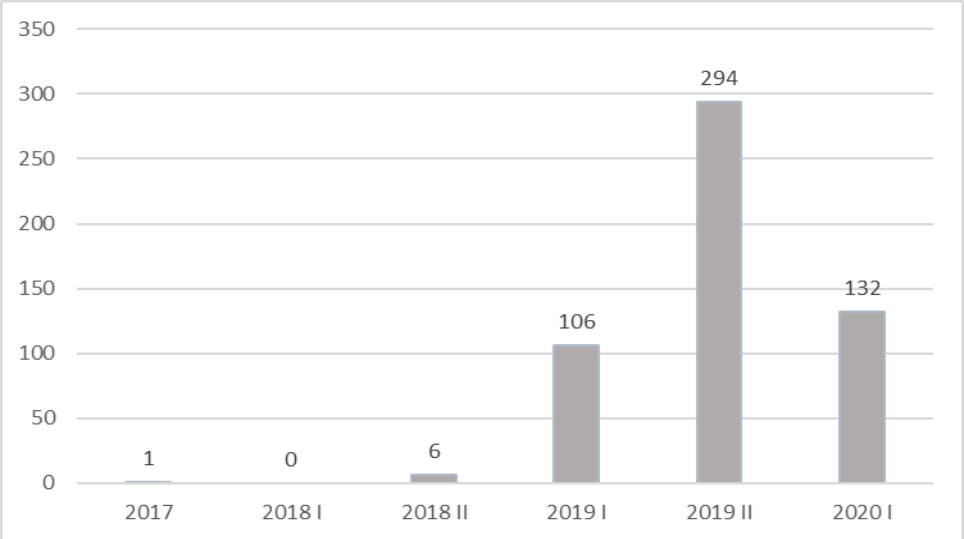

Diagram 7. The number of the reports sent to the *RAB* and the dynamics in 2017–2020 per semester

In 2019, the reports sent by providers of a virtual currency service formed 5,7% of all the reports received by the *RAB*, but even 93% of the relevant reports were sent by only three entrepreneurs. Out of all the VC enterprises that had started business in Estonia, less than 6% (16 out of 280) sent reports. Out of that can be concluded that in the VC sector the obligation to notify and to apply due diligence measures is obviously inadequately lived up to. Most often, the notification that was sent at entering into a customer relationship, but also during a customer relationship, concerned a suspicion of false documents. The notifications show the fact that only a very small share of the enterprises monitors the movement of crypto-currency even on the basis of public transactions. The inadequate fulfilling of the obligation of reporting is also confirmed by the answers of the questionnaire where most of the enterprises noted that they have refused transactions entering into a business relationship or occasionally a transaction. According to § 49 of the Money Laundering and Terrorist Financing Prevention Act, there is also a duty to report to the *RAB* about those facts, a duty most often neglected. The *RAB* has referred only a small number of the notifications that have been sent to *RAB* by VC service providers further to be thoroughly analysed, as the majority of the persons about whom the reports have been sent, has not a connection to Estonia whatsoever.

---

[21] One fifth of the providers of a wallet also use external service providers to create wallets.

The translator Kristi Ugam is aware of the requirements of the [Estonian] Code of Criminal Procedure (*KrMS*) § 161 and of the responsibility laid down in § 321 of the [Estonian] Penal Code (*KarS*) (signed digitally).

Also, the supervisory unit of the *RAB* estimates that there are shortcomings in fulfilling the obligations of application of due digigence measures - that in case of identity checks as well as in case of monitoring a business relationship. In the framework of supervisory activities, it has appeared that during identity checks enterprises have accepted documents that do not compy with the requirements, for example internal documents of a foreign country, that are not valid travel documents[22]. As the method to check the identity of the customers is usually to check from a distance/a remote check, and the data presented are often not varified by means of information technology, the service providers should apply extra due diligence measures when checking the identities of persons (§ 38 of the MLaTFA), for example they should demand additional documents. Service providers who use remote identity check, often fail to fulfill that duty, using only one document to identify a person (e.g. a passport). The situation should be imporved by the more strict rules for identification of persons, introduced by the amendments to the Money Laundering and Terrorist Financing Prevention Act, that entered into force in March 2020: in addition to presenting an identification document of a person the data of citizens of third coutries must be varified by means of information technology, provided one is not situated in the same place together with the customer or his/her representative.

The supervisory unit of the *RAB* has also noticed that VC entrepreneurs monitor business relationships inadequately, to be precise, one does not apply the enhanced due diligence measures laid down in § 38 of the Money Laundering and Terrorist Financing Prevention Act, for example one does not reassess the customer´s risk profile not later than six months after the establishment of the business relationship.

2.4 The geographical risk of providing a service of a virtual currency

During the analysis it turned out that the owners and board members as well as the addresses of the registered offices of many enterprices that provide a service of a virtual currency are the same. For example, at end of February 2020, there were 135 enterprises with a valid operating licence for providing the service of exchanging VC for money, that had one and the same house at the Peterburi road as their registered office; the registered office of 54 enterprises was an appartment at the Pärnu road, and 50 enterprises had their registered office in an appartment at the Punase street. In total, 20 addresses were discovered in the framework of the inquiry that are noted as the registered office of at least 10 providers of the service of exchanging a virtual currency for money. These 20 addresses were registered offices for 624 i.e. more than half (57%) of all the providers of the service of exchanging a virtual currecy for money. A similar outcome appears in case we look at the addresses of the places of business: for 190 enterprises that had an operating licence for providing the service of exchanging VC for money with the stand of the end of February 2020, there was one and the same house at the Roosikrantsi street registered as the place of their business; as the place of business of 133 enterprises, a building at the Peterburi road was registered.

The results of the analysis also show clearly that a remarkable share of the enterprises that possess an Estonian operating licence for providing a VC service have their actual business activities abroad and there is no connection to Estonia. That is indicated by an analysis of the websites of the providers of virtual currency services (the contact information there and the representatives are as a rule foreign), by the data of the Commercial Register (there is no turnover and there are no employees in Estonia) as well as by an analysis of the reports of VC service providers to the Financial Intelligence Unit (in majority the reason for sending a report is a suspicion of an identity theft concerning a person that does not

[22] The requirements are laid down in § 21 of the Money laundering and Terrorism Financing Prevention Act.
The translator Kristi Ugam is aware of the requirements of the [Estonian] Code of Criminal Procedure (*KrMS*) § 161 and of the responsibility laid down in § 321 of the [Estonian] Penal Code (*KarS*) (signed digitally).

have a connection to Estonia). In the framework of the analysis, a connection between the enterprise and back-ground countries as Russia, Latvia or another East-European appeared and the enterprises were often connected by concrete providers of the service of an Estonian enterprise that operated as a link that made it possible for numerous foreign service providers to appy for an Estonian operating licence. In case of the largest service providers (at least 1 million euros of turnover of the mediated services in 2018 or in the first half of 2019), less than 5% (2 service providers out of 43) could be identified as having actual business activities and owners in Estonia. 40% (17) of them noted in the questionnaire that they have employees in Estonia.

The data about the location of the holding accounts of the VC service providers also refer to little connection of the enterprises to Estonia. Almost 40% of the enterprises had their holding account in Lithuania at the moment of answering the questionnaire, 25% had theirs in Great Britain and 10% in Estonia. Enterprises have had a greater interest in opening an holding account in Estonia, but according to the information that has reached the *RAB*, one may claim that banks are not eager to accept them as customers. The *RAB* has also received information that due to that, private persons have tried to close out transactions of an enterprise on his/her private bank account. The *RAB* has also been informed about attempts of strawmen to open an holding account for VC service providers.

The risk of reputation loss of the Estonian sector of virtual currency is increased by a considerable connection to e-residents. According to the data of the Comercia Register, with the stand of February 2020, 36% of the providers of a virtual currency wallet and 35% of the providers of the service of exchanging a virtual currency for money had at least one e-resident as an associated person (contact persons excluded). In total, there are 554 former or present e-residents that have been associated with providers of a virtual currency service.

In the framework of the questionnaire of the *RAB*, enterprises were also asked to present the number of consumers of their service per country. It turned out that the majority of services were provided for citizens of The United States of America that formed slightly more than one tenth of all the consumers of the service in the period 01.01.2018–30.06.2019. Somewhat surprisingly, Venezuela followed in that classification with a bit less than one tenth, but that was greatly due to the clientèle of a large company. Citizens of Vietnam, Russia, Brazilia and Indonesia formed (separately) *ca* 5% of all the consumers of the service. More than 2% of all the consumers of the service came from India, Iran, Great Britain, China as well as from Japan. Only *ca* 0,15% of all the customers of the service providers with an Estonian operating licence come from Estonia.

To conclude, among the owners as well as customers of VC enterprises there is a great number of persons that come from countries with a greater geographical risk in the sense of the Money Laundering and Terrorist Financing Prevention Act § 37 subsection 4. The problems of the lack of connection to Estonia of the enterprises with an operating licence and a more efficient identity check were addressed by the law amendment previously mentioned that entered into force on March 10, 2020. Taking the vulnerabilities of the VC sector into consideration, the generally low level of due diligence of the service providers included, it is still likely that the measures that have been taken up to now cannot sufficiently mitigate the geographical risks of money laundering and terrorist financing that are connected to the VC service providers.

The translator Kristi Ugam is aware of the requirements of the [Estonian] Code of Criminal Procedure (*KrMS*) § 161 and of the responsibility laid down in § 321 of the [Estonian] Penal Code (*KarS*) (signed digitally).

3 The risk of criminality that is associated with virtual currencies

Many significant risks involved in virtual currencies have brought along a necessity to regulate new technologies from the point of view of the money laundering and terrorist financing prevention. Virtual currencies have received much attention as an innovative instrument of payment as well as as an easy opportunity for criminals to move and store illegally obtained assets out of reach of law enforcement institutions[23]. Virtual currencies can be used as means of payment, but also for example as an exchange instrument, for investment, as products of maintaining a value or in internet casinos. In the point 9 of the preamble of the Directive (EU) 2015/849 the following is acknowledged:

> *The anonymity of virtual currencies allows their potential misuse for criminal purposes. The inclusion of providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers will not entirely address the issue of anonymity attached to virtual currency transactions, as a large park of the virtual currency environment will remain anonymous because users can also transact without such providers.*

Many characteristics of virtual currencies, such as the complications identifying the beneficiary or in some cases also the impossibility of it, the convenience, speed and cheapness of international transactions, and in some cases the lack of intermediaries, complicate criminal proceedings and confiscation of assets[24]. Virtual currencies afford criminals to deposit assets outside the formal financial system and digitally in order to hide the origin and final acquirer of them. Virtual currencies can be used in the phase of committing a predicate offence as well as in the money laundering phase. It is known that virtual currencies are often used to commit fraud, a part of such crimes being of a very large scale[25]. In addition to that, virtual currencies are used for paying for illegal activities as well as for exchanging the proceeds of crime[26].

Virtual currencies play a growing role as a payment instrument in the dark web, that affords criminals to trade in a hidden way in anything from weapons to narcotics. Particularly in the trade of narcotics the use of virtual currencies have been clearly noticed in the past years. In 2016, as a result of an international investigation, ten people were arrested in the Netherlands who were associated with laundering the money earned by selling Ecstasy; they were using Bitcoin for that[27]. In 2018, the leader of a group trading in narcotics was sentences to jail for 11 years in the United States of America, whereas the selling activities of the group took primarily place through the dark web and Bitcoin[28]. According to

---

[23] FATF. (2014). *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*. FATF, Paris, France. http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html

[24] FATF. (2014). *Virtual Currencies* ja Elliptic. (2019, July 29*). Bitcoin: Anti-Money Laundering Challenges and Solutions*. Bitcoin Magazine. https://bitcoinmagazine.com/articles/bitcoin-anti-money-laundering-challenges-and-solutions

[25] For example, since the year 2017, there is a person in custody in Greece and France under suspicion of embezzlement of Bitcoins approximately in the value of 4 billion USD, obtained through large-scale hacking and computer fraud. – https://www.theguardian.com/technology/2017/jul/27/russian-criminal-mastermind-4bn-bitcoin-laundering-scheme-arrested-mt-gox-exchange-alexander-vinnik ja https://www.coindesk.com/france-charges-alleged-btc-e-operator-alexander-vinnik-following-greek-extradition

[26] Keatinge, T., Carlisle, D., Keen, F. (2018). *Virtual currencies and terrorist financing*.

[27] https://www.theguardian.com/technology/2016/jan/20/bitcoin-netherlands-arrests-cars-cash-ecstasy

[28] https://www.denverpost.com/2018/09/27/ecstasy-trafficking-ring-belgium-colorado/

The translator Kristi Ugam is aware of the requirements of the [Estonian] Code of Criminal Procedure (*KrMS*) § 161 and of the responsibility laid down in § 321 of the [Estonian] Penal Code (*KarS*) (signed digitally).

a study from the year 2018, approximately a quarter of the users of Bitcoin is connected to an illegal activity and almost half (46%) of the transactions of Bitcoin are connected to crime[29].

3.1 Money laundering risks that are specific for virtual currencies and mitigation of those risks

According to the estimation of Europol, 3–4% of the illicit proceeds laundered in Europe are done so with the help of virtual currencies[30]. The investigation unit of the United States Congress discovered that in the years 2009–2018 on the main VC markets there was Bitcoin used for laundering assests in the value of 2,5 billion USD at a rough estimate; that is a fraction of the transactions on the world scale though, and the volume is increasing continually[31].

VC wallets are very easy to create, it is also uncomplicated to share even large sums among many parties, that makes it difficult to discover money laundering schemes if virtual currencies are involved. There are also virtual currencies with extended anonymity (AEC) that, according to FATF (Financial Action Task Force), remarkably reduce the possibilities of VC service providers to monitor the services and to take due diligence measures to customers[32].

Criminals understand that it is possible to monitor the movements of the virtual currencies that use blockchain technology (for example Bitcoin, Ethereum), the reason why so-called mixers or tumblers are used: an illegally obtained virtual currency is mixed with a legitime one that makes the monitoring of the movement of the assets considerably more complicated, if not impossible[33]. Mixers bring also a risk of fraud along as there are cases known where mixers have embezzled partly or fully the assets that are in virtual currency of their users[34].

Mixers can, similarly to virtual currencies, be dividend into centralized and decentralized. Typical centralized mixers use two transactions and four VC addresses:

A: the address of the use, where the criminally obtained assets come from;
B: the address of the mixer, where the user deposits his/her assets;
C: the address of the mixer, from where assets of a third party are sent to the user;
D: the address of the user, where laundered assets arrive.

In the first transaction of ordinary mixings a user sends the VC-s from his/her account A to an address B of the mixer. The mixer deducts the service charges and transfers the rest of the sum, as the second transaction, from its second address C to the second address D of the user. There is no direct connection between A and D, the reason why the precise origin of the asset is later very difficult to identify.

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

[30] https://www.bbc.com/news/technology-43025787

[31] Sykes, J. B., Vanatko, N. (2019). *Virtual currencies and money laundering: legal background, enforcement actions, and legislative proposals.* Congressional Research Service.

[32] FATF. (2019). *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. FATF, Paris. www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html

[33] Haffke, L., Fromberger, M., Zimmermann, P. (2019). *Virtual Currencies and Anti-Money Laundering.*

[34] Europol. (2018). *An Introduction to Bitcoin Mixers.*

Decentralized mixings associate several transactions; as a result, it is later not possible to identify precisely whose assets went where[35].

Critics have pointed out that the greatest weakness of the Directive (EU) 2015/849 is that the Directive does not regulate mixers, the reason why those intermediaries are not obliged to take the due diligence measures of prevention of money laundering and terrorist financing[36].

FATF (Financial Action Task Force), a transgovernmental organisation that develops standards for combatting money laundering and terrorist financing, emphasizes that the measures for money laundering and terrorist financing prevention of countries should be risk-based. Accoring to the estimation of FATF, the measures concerning virtual currencies should concentrate on the exchange points of virtual currencies and money, where the risks connected to virtual currencies and the need for transparency are the greatest. As an extra risky place, the study of FATF points the ATM-s of VC out, as there is no efficient supervision over them. According to the estimation of FATF it is likely that if the degree of regulation of the VC service providers (virtual asset service providers, abbreviated VASP) increases, the use of exchange mechanisms from person to person (the so-called P2P) and decentralized intermediaries increase, that makes controlling for law enforcement institutions significantly more difficult[37].

In 2019, FATF corrected its standards, introducing a requirement for countries to assess and mitigate the risks concerning virtual currencies. To do that, countries need to licence or register providers of virtual currency services. Countries should guarantee that providers of the service use all possible prevention measures for money laundering and terrorist financing, including the due diligence measures concerning a customer, gathering and storing of the data of customers and transactions, reporting suspicious transactions and making sure that the transactions would comply with international sanctions. In addition to that, service providers should be monitored and punished if necessary, in case providers of services do not apply the due diligence measures of money laundering and terrorist financing prevention. It was also specified that following the recommendations of FATF, virtual currencies should be treated as assets, profit or another analogous unit of value[38].

The Estonian regulations have in majority been adapted to the standards mentioned of FATF. Whereas the licencing of VC service providers on the basis of an operating licence was in use in Estonia already previously, as well as the obligation to report and the obligation to gather and store the data of customers and transactions, the law amendment that entered into force on March 10, 2020 addressed many recommendations of FATF. For example, the instructions of FATF point out that VC service providers should be licenced exactly in their place of business. Even though the VC service providers in Estonia were obliged to apply the due diligence measures already before the law amendment, it was not possible to practice efficient supervision over enterprises that operate mostly abroad and to apply enforcement measure before the renewal of the regulations. Also the requirement of a correct business reputation of an entrepreneur that wishes to provide a VC service, a requirement added in March, is in connection to the instructions of FATF (countries should take preventive measures, so that legal bodies

---

[35] *Idem.*

[36] Haffke, L., Fromberger, M., Zimmermann, P. (2019). *Virtual Currencies and Anti-Money Laundering.*

[37] FATF. (2019). *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*.

[38] FATF. (2019). *Public Statement on Virtual Assets and Related Providers*. FATF, Paris. http://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html

The translator Kristi Ugam is aware of the requirements of the [Estonian] Code of Criminal Procedure (*KrMS*) § 161 and of the responsibility laid down in § 321 of the [Estonian] Penal Code (*KarS*) (signed digitally).

could not be used for monley laundering/terrorist financing, through identifying the actual beneficiary and through control). In comparison to most of the member states of the European Union, Estonia has also regulated, on the basis of the recommendation of FATF, exchanging a virtual currency for a virtual currency. In addition to that, the RAB started in 2020 to give written feed-back to its duty holders about fulfilling the duty to report; in the framework of that all enterprises possessing a VC operating licence received a feed-back report about the VC sector.

In the VC sector there is no reporting obligation concerning the data that characterize providing the service, introduced neither on the level of Estonia nor of the European Union; due to that, the sector is characterized by a non-transparency of the parties of transactions. Even though transactions are public and can be followed, it is not easy to identify persons behind wallet addresses nor their physical location, not to mention the original origin of the assets concerned. As the Estonian credit institutions have not been eager to open holding accounts for enterprises that provide a VC service, the *RAB* does not receive too many reports from them on suspicious activities of VC enterprises either. A great responsibility identifying suspicious transactions falls on the VC service providers, whose application of due diligence measures has been inadequate up to now or who have now and then neglected the obligation deliberately.

3.2 The risk of terrorist financing connected to virtual currencies

Some experts have estimated though that virtual currencies constitute a higher risk in the context of money laundering and a lower risk in that of terrorism,[39] but it is likely that the risk of virtual currencies in connection to terrorist financing is being underestimated. Virtual currencies are administered in a decentralized way, they are easy to use and transactions can be made relatively quickly; at the same time, there are loopholes in the international regulation and the regulation is inadequate, and it is difficult for law enforcement institutions to get information from service providers. It is not credible that VC-s are not widespread for terrorist financing while they are so widely in use in criminality.

According to the estimation of the official of the Estonian Internal Security Service who gave an interview, VC-s are more and more wide-spread among Islamic extremists who use them for organizing money raising campaigns, sharing anonymous wallet addresses through social media or communication applications. Such campaigns were organized by ISIS/Da'esh but they are used today too, among others to support the armed groupings of the area of Idlibi or the families of foreign combatants who live in refugee camps. It is also known that virtual currencies are used, more than earlier, among Palestinians to finance the armed conflict of the territory administered by the Palestinian National Authority with Israel. The only things that hinder a very widespread exploitation of virtual currencies for terrorist financing are the great fluctuation of the exchange rate of the crypto-currency and limited possibilities to exchange VC for money.

The volatility of virtual currencies does not change them into a reliable instrument of moving or storing assets and the more widespread crypto-currencies like Bitcoin do not offer ultimate anonymity, but technological developments can change it. There is a relatively small number of confirmed cases of terrorist financing by means of virtual currencies, but there are more and more cases of discovering with hindsight that certain virtual currency transactions could have been connected to terrorist financing. There are cases identified where Islamic or right extremist groupings have used virtu al currencies to

[39] Keatinge, T., Carlisle, D., Keen, F. (2018). *Virtual currencies and terrorist financing*.

purchase illegal objects from the dark web (e.g. weapons), to raise capital from crowdfunding platforms or to move assets internationally (P2P i.e. transfers from person to person).

The use of virtual currencies of greater anonymity, like Monero, has increased and gained influence, but as they are not easy to exchange for cash they are not very widely used among extremists. The higher risks of terrorist financing of the future concern a possible convergence of cybercrimes and the use of crypto-currencies. For example, North Korea managed to raise Bitcoins in the value of 140,000.00 USD by the WannaCry cyberattack and the country has been associated with organizing other cyberthefts too[40].

There is also information about Estonia concerning the use of virtual currencies for terrorist financing. For example, an Estonian citizen who was in the business of mediating virtual currencies (P2P transactions) without an operating licence made transfers in 2017 to a person who was also in the business of mediating virtual currencies and who was connected to financing a terrorist organization in East Asia. The Estonian mentioned was, to be sure, not aware of the connection, but the case shows, in what one can unwillingly become involved by trading in non-transparent VC. The *RAB* has also received reports from service providers informing about sanctioned persons who are involved in terrorism wanting to enter into business relationships, a fact that certainly indicates an attractiveness of virtual currencies for terrorist financing.

3.3 The use of virtual currencies in the Estonian crime

An investigator of cybercrimes at the Estonian Police and Border Guard Board who gave an interview in the framework of the present inquiry, pointed out that using virtual currencies in criminal schemes is common in Estonia; a great deal of the so-called bill-presentment and payment of the criminal environment takes place in virtual currencies, and a lot of virtual currencies are also used in the preparatory phase of crimes. From the point of view of cybercrimes, virtual currencies are used in case of almost all sorts of crimes; according to the investigator of cybercrimes, it is not possible to point out one or a couple of dominant sorts of crime, but it is very common that one pays for example for all sorts of infrastucture that is used for criminal purposes (e.g. the control servers of malware) or for criminal services (e.g. purchasing stolen data, source code of malware) using virtual currency as a payment instrument, but it is also common to ask a ransom in crypto-currency.

The Central Criminal Police sees primarily two risks in connection to virtual currencies: 1) the risk of fraud (often in connection to investments) and 2) the risk of money laundering.

The risk of fraud holds a more prominent place, as by now there are more practical examples about that: Estonia has received a great number of letters rogatory in cases where providers of VC services have committed fraud.

The use of virtual currencies for money laundering has been confirmed through cooperation of legal assistance as well as through the Estonian criminal proceedings.

In November 2019, the sentence of The Viru County Court in a case of computer fraud entered into force: the convicted person had used virtual currencies to hide the traces of criminally obtained money[41].

---

[40] *Idem*.

[41] The Sentence of the Viru County Court No 1-19-5363
The translator Kristi Ugam is aware of the requirements of the [Estonian] Code of Criminal Procedure (*KrMS*) § 161 and of the responsibility laid down in § 321 of the [Estonian] Penal Code (*KarS*) (signed digitally).

That is the first case in Estonia of using virtual currencies for money laundering that has reached the judgement. The scheme was, summarized, the following.

SG contributed to different cases of computer fraud that were committed abroad. For that SG recruited straw-men in Estonia, who, following his/her[42] instructions, opened holding accounts in different banks in Estonia and concluded contracts of using the service of internet banking. The strawmen gave the access information of the bank cards and bank accounts through SG to the person(s) who committed the computer fraud (the persons who committed the fraud were not identified in the scheme), who, at their turn, opened on the basis of that access information accounts in virtual payment systems and banks as well as formalised virtual payment cards. Subsequently, a criminal/the criminals gained access to the data processing of different countries and in the bank, they transferred money from bankaccounts of the customers to the holding accounts of the recruited straw-men in Estonia in total for a sum of more than 50,000 euros.

In order to contribute to the cases of computer fraud, SG recruited RA to help him/her, who gave SG advice about virtual currency transactions. RA offered SG an access to his/her virtual wallets and administerd the virtual wallets of SG. RA also made transfers in favour of SG to the holding accounts of third persons and him-/herself, using different virtual payment intruments and crypto-currency. The relevant scheme is depicted on the diagram 8.

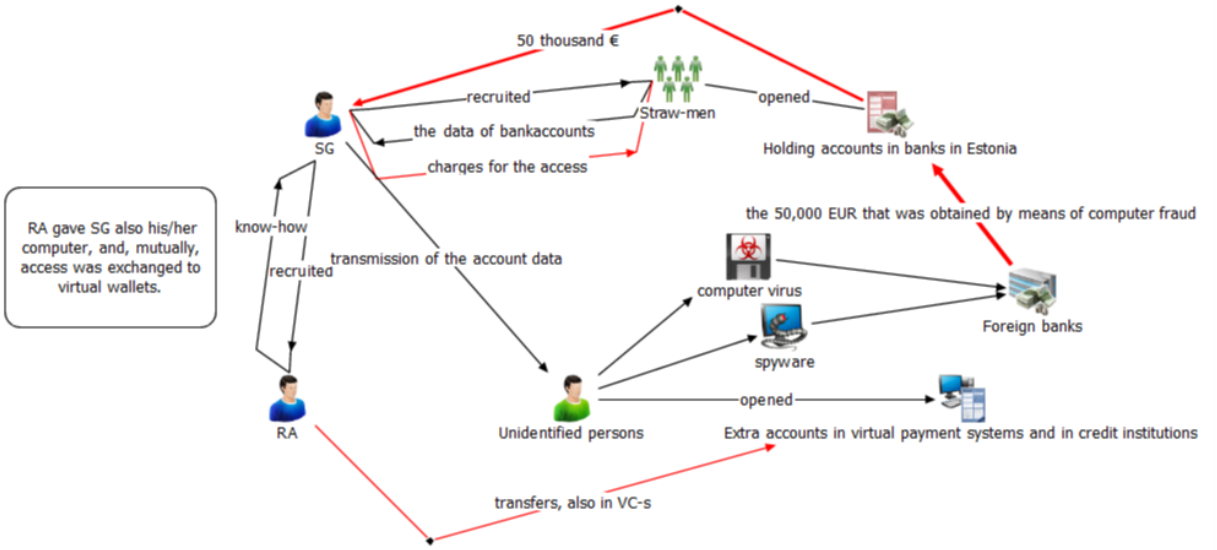

Diagram 8. The money laundering scheme that reached a conviction.

In the time of writing the present inquiry, a case has reached the conviction in the Court of First Instance but the sentence has not yet entered into force: the cybercrime unit has discovered an in 2016-2018 committed possible laundering of crypto-currency in the amount of 3 million euros. The scheme of the case was the following:

[42] The natural person referred to has most probably one certain gender identity known to the writer of the text, but from a written Estonian text that only uses pronouns, it is not possible to conclude whether the person is male or female. (translator)
The translator Kristi Ugam is aware of the requirements of the [Estonian] Code of Criminal Procedure (*KrMS*) § 161 and of the responsibility laid down in § 321 of the [Estonian] Penal Code (*KarS*) (signed digitally).

The accused searched in internet databases for leaked-out user names and passwords of people, trying to use them for entering into all kinds of wallet and e-mail services. In case of success he/she transferred the assets obtained to the accounts of crypto-currency that were under his/her control, from there he/she made different transactions. He/she transferred a part of the money to casinos that accept crypto-currency and that did not care to identify the origin of the money, and when the person won something in those environments, the money was transferred from the casino back to the provider of the wallet service, who, if necessary, converted it and transferred it as a SEPA [single European payment area] payment to the bank account. In addition to that, the person used bank cards of a service provider from the origin of Gibraltar, that made it possible to use crypto-currency for payments as credit. The person transferred a part of the monetary means to the bank accounts of his/her acquaintances in order to get it into his/her possession in the form of cash.

There are also several examples in the practice in Estonia of using virtual currencies for trading in narcotics. The criminal court is presently proceeding the following case:

The person is accused of handling various narcotic substances in large quantities in the value of many hondreds of thousands of euros. More precisely, the accused is suspected to have sold narcotic substances (Ecstacy, LSD, amphetamine and such) on various platforms of the dark web whereby mainly crypto-currencies (Bitcoin, Monero) were used for purchasing as well as for reselling them. For delivering the narcotics, usually hiding places in the nature were used or sending by post. In the framework of the seizure of assets, in addition to cash and holding accounts, also Bitcoins as well as Monero tokens from the virtual currency wallets of the person were confiscated.

According to the representative of the unit of digital criminalistics of the Central Criminal Police who was interviewed, the first expose of the unit to virtual currencies in the framework of a criminal proceeding was in 2017. By now, more than 30 Bitcoins have been frozen in the framework of approximately ten proceedings, but also other currencies have passed in proceedings, like Monero. In one case the currency has also been returned after it had been deposited at the police.

The investigator of cybercrimes who was interviewed pointed out that using virtual currencies depends on the scale of the scheme. In the simpler criminal schemes people are deceived or blackmailed to part with their virtual currencies, these will then be transferred to the wallet of the criminal, and to cover up the traces, the money is "spinned" around. If the quantities are large, it is common that an employee of an enterprise that provides a VC service is involved, whereas the employee overlooks the requirements of money laundering prevention. What complicates the investigation of deceiving and blackmailing schemes is the fact that criminal profits are transferred into countries where the VC regulation is weak, it is not possible to get information and it is not possible any more to follow the movement of the money. According to the person interviewed, a considerable share of ICO-s is done with the purpose of money laundering. It is also telling about the environment of crypto-currency that a small group of people controlls the majority of the calculating capacity. The easier it is because of that to exploit crypto-currencies also in money laundering schemes and to agree with each other who is mining at a certain moment and who is not.

Law enforcement institutions have discovered that several dark web environments are connected to Estonia, that do not fulfill the requirements of money laundering prevention and where money of

criminal origin is moved. There are also examples whereby the Estonian law enforcement institutions have intervened in time to prevent creating such environments.

Talking about trends, the interviewed investigator of cybercrimes pointed out that the tempo of the increase in using virtual currencies in criminal schemes has stabilized. The person was of the opinion that the reason for that is not so much that people would be more aware and able to protect themselves, but that the environment is used up to a certain extent: certain sorts of crime where virtual currencies are used, have taken root, and new ones have not appeared.

For investigation of cybercrimes, from the point of view of virtual currencies, the most important concern is international cooperation: cooperation with certain countries does not work; that makes discovering of schemes and prevention of crimes complicated, considering that almost all the cases have an international scope.

According to the experts of digital criminalistics of the Estonian Police and Border Guard Board (PPA), the number concerning proceedings of virtual currencies is growing, but the relevant skills of the investigators are inadequate for proceeding; for example, one is not aware of the opportunity to ask service providers for information. A bottleneck is the legislation as well as the internal regulations of the *PPA* that do not describe exactly the freezing/confiscating of virtual currencies. At the moment it is simply a matter of agreement, the person subject to proceedings is offered an opportunity to deposit the currency to the crypto-currency account of PPA or to convert it to euros. Another problem is that in the resolutions of the court sentences, the value of virtual currencies is noted in euros, not in the quantity in the crypto-currency: because of the very great volatility of virtual currencies, it is a wrong practice.

3.4 Data processed by the RAB and measures for mitigating risks

Neither taking the reports of VC service providers themselves in consideration, nor the information that has been received through international cooperation, the *RAB* has received approximately 150 reports in the period of 2015 until April 2020 where crypto-currencies are mentioned in one way or another. In the years 2018-2019, the *RAB* has received almost 30 international information requests.

The *RAB* has received a great number of reports of fraud that is connected to virtual currencies, more often than not they concern investment fraud. For example, enterprises with an Estonian operating licence have in many cases used a simple "exit scam" i.e an exit fraud, whereby the customer does not get an opportunity to transfer his/her assets away from the service provider and the assests will be embezzled. There are victims from very different countries, one finds them from Bulgaria up to the Marshall Islands, but of course also from Estonia, whereas the enterprises that have organized the fraud are typically having East European owners. In the framework of the external cooperation of financial intelligence units it has been discovered that a couple of large-scale exit-scams have also involved enterprises that are registered abroad and that are directed by e-residents of Estonia.

A repeated pattern of investment fraud has happened so that customers have been approached by telephone or by phishing e-mails offering them a good investment opportunity and convincing them to download a remotely controlled software in their computer. Subsequently, in the name of the victims for example instant loans have been taken, that have been immediately transferred to crypto-currency platforms, or in connection to their bankaccounts virtual cards have been made that were used to make BTC payments at the expense of savings. Several such cases have also reached court proceedings.

The translator Kristi Ugam is aware of the requirements of the [Estonian] Code of Criminal Procedure (*KrMS*) § 161 and of the responsibility laid down in § 321 of the [Estonian] Penal Code (*KarS*) (signed digitally).

The characteristics of a typical fraud according to the information that has reached the *RAB* are the following:

The intelligence leads that the *RAB* has rather often received about transfers of the money that is obtained in a criminal way, for example by trading in narcotics or business letter fraud, into virtual currencies, show that VC-s are a promising and frequent way of money laundering. Also, in many cases, in the banks operating in Estonia the movement of unsuitably large amounts of money for the profile of the customer, whereby the assets have come from virtual currencies and the customer has not been able to substantiate the origin of the assets convincingly, have risen suspicion – that can refer to an illegal VC exchange service or also to money laundering.

The *RAB* has also received information from law enforcement institutions abroad about the connection of Estonian enterprises or e-residents to organizing suspicious ICO-s and embezzlement of large sums in the framework of them. A frequent association of ICO-s with criminality is clearly a problem that cannot efficiently be addressed by the present legal order, as it is not completely clear whose duty it is to conduct supervision over them. On the international level ICO-s are usually unregulated[43]. Publicly advertised ICO-s often become targets of cyberattacks. In 2018, Ernst & Young published a study according to which nearly 10% of the money gathered by means of ICO-s is stolen during hacking, often by phishing letters[44].

In the past years, the supervision activities of the *RAB* have concentrated greatly on the sector of virtual currencies. As the majority of the owners and board members of the service providers that have applied for an Estonian operating licence are citizens of foreign countries, who do not have an actual place of business in Estonia, the method of remote control has been widely applied for conducting national supervision. In 31 cases of the 34 of the supervision proceedings that were conducted in the year 2019, it was discovered that the enterprises had not started business activities in Estonia, and their operating licences were declared null and void. In many cases there was previous negative information about the given enterprises, for example a suspicion of fraud. Paying extra attention to the sector is also in the future one of the priorities of the supervision activities of the *RAB*.

---

[43] Blandin, A., Cloots, A. S., Hussain, H., Rauchs, M., Saleuddin, R., Allen, J. G., ... & Cloud, K. (2019). Global cryptoasset regulatory landscape study. University of Cambridge Faculty of Law Research Paper, (23).

[44] https://www.information-age.com/10-ico-funds-stolen-ey-123470528/

The translator Kristi Ugam is aware of the requirements of the [Estonian] Code of Criminal Procedure (*KrMS*) § 161 and of the responsibility laid down in § 321 of the [Estonian] Penal Code (*KarS*) (signed digitally).

The law amendment that entered into force in March 2020 is a step in the right direction, but the *RAB* is of the opinion that keeping in mind the severe crimes of the branch, the requirements for VC service providers should be made even more strict and extra [financial] means should be spent on the supervision of the sector (IT-solutions and increasing the number of supervising officials). Risks can be mitigated by introducing an obligation to hand in regular reports on the transactions, turnovers and customers of the VC enterprises. In such a way, the *RAB* would get a much better overview of the market participants. Information about in what a scope and on which markets the enterprises that fall under the supervision, operate, enables, among other things, to estimate where the risks of the VC sector concentrate themselves. Comparing the given information to the other information that the *RAB* receives, would also give an opportunity to estimate remarkably better how well VC enterprises fulfill their obligation of due diligence. In addition to that, issuing the operating licence, the business plan of the enterprise could be used as a check-object. The business plan should include a plan for a system of transaction monitoring and a plan for fulfilling the duty of "know your client" (KYC). It should also be a prohibited for VC service providers to make transactions, if fulfilling the duty of taking due diligence measures is impossible or significantly complicated.

In the "Intention to develop a regulation for crypto-assets" that was published in November 2019 it is pointed out that at the moment, as far as virtual currencies are concerned, there are no legal guarantees that accompany regulated financial services and investments, the reason why the customers of the services may not get access to their assets any more, if the platform faces for example business problems or a cyberattack[45]. The *RAB* supports the proposition to create an additional regulation for protecting persons and their virtual assets. The present money laundering prevention requirements do not help sufficiently to combat unprofessionality of service providers or cases of fraud that are rather regular phenomena in the sector. Requirements for information systems, for cybersecurity, but also for the structure of an organisation, and the guarantees that the assets of persons would be preserved, would help to mitigate the risks considerably. The requirements for service providers for handling and storage of data should be clearly defined; that would simplify the protection of the rights of persons as well as conducting supervision. While planning a regulation of virtual assets one should consider the risk that service providers give customers untrue price information or manipulate the transaction prices, participating in the transactions themselves[46]. In the framework of the proposed additions, it would be a logical step to subject VC-s to financial supervision.

[45] https://www.rahandusministeerium.ee/sites/default/files/news-related-files/kruptovarade_reguleerimise_vtk.pdf
[46] *Idem*.

4 Summary

In connection to the large number of providers of virtual currency services, that are registered in Estonia, to their loose connection to Estonia, and to the non-transparency of the services, the sector of virtual currencies constitute a great risk of crime, including money laundering, and of reputation loss for Estonia. Thereby, the legal framework has in majority not corresponded to the risks.

In the past years, the number of the cases of fraud and suspicion of money laundering has been increasing. Using virtual currencies in criminal schemes is widespread in Estonia, a great deal of transactions of the criminal environment take place in virtual currencies and also in the preparatory phase of crimes virtual currencies are widely used. Cases of drug trade that are connected to virtual currencies are numerous, a number of them have reached court proceedings. In Estonia, also the risk of fraud is prominent (often in connection to investments) as well as the risk of money laundering. The *RAB* has received reports on cases of different investment fraud (including exit-scam), but also on the use of virtual currencies (including organising ICO-s) for money laundering. One must also not underestimate the risk of terrorist financing associated with the VC sector. The anonymity, easiness and speed of the VC transactions, while law enforcement institutions are in difficulties getting information from enterprises and exchanging information internationally, give reason to suspect that VC-s are an attractive instrument for terrorist financing.

The first operating licences in Estonia for providing a service of virtual currencies was issued at the end of the year 2017. While the number of the operating licences issued was modest in the first year, then the number of the VC service providers who had applied for an operating licence in Estonia increased very rapidly in the years 2018-2019. In the years 2017–2019, 1250 operating licences were issued for the service of exchanging VC for money and 1140 operating licences for providing a VC wallet. The business activites of the enterprises with an operating licence took usually place abroad and the owners and customers were in majority foreigners.

During the background analysis of enterprises the *RAB* discovered that out of the 44 biggest service providers (the turnover of the service provided in the first half of the year 2019 was at least 1 million euros) the location of the actual business activity and the owners of only two enterprises was in Estonia. The background of the majority of the VC enterprises turned out to be that of Latvia, Russia or another East European country. Analysing the data of the associated persons of all the enterprises it was discovered that there was at least one e-resident behind almost one third of the enterprises.

According to the data of the questionnaire, the share of Estonians among all the consumers of VC services was only 0,15%. The greatest number of the customers of the services provided had the citizenship of the United States of America (10,4% out of all the consumers of the services), to be followed by citizens of Venezuela (9,3%), Vietnam (6,2%), Russia (4,9%), Brazilia (4,3%), Indonesia (4,1%), India (2,6%), Iran (2,5%), Great Britain (2,2%), China (2,1%) and Japan (2,1%). The *RAB* discovered during the analysis also that the owners and board members of many VC service providers were the same, as well as the legal addresses of the enterprises.

The generally loose connection to Estonia of the VC enterprises with an operating licence has made supervision complicated as well as the proceeding of cases with traits of crime. The duty to report to the *RAB* has also been fultilled inadequately by VC service providers. Out of all the the VC enterprises who had started business activites in Estonia, less that 6% sent reports to the *RAB* in 2019 (16 out of 280), that is a clear indicator that in majority the enterprises of the sector do not take the due diligence measures correctly or they do not take them at all. That is also confirmed by the answers of the service The translator Kristi Ugam is aware of the requirements of the [Estonian] Code of Criminal Procedure (*KrMS*) § 161 and of the responsibility laid down in § 321 of the [Estonian] Penal Code (*KarS*) (signed digitally).

providers in the questionnaire and by the results of the supervisiory proceedings of the *RAB*: the due diligence measures taken are evidently insufficient in the field of identifying the persons of the customers of the service as well as of monitoring of business relationships.

Important amendments in the regulation concerning virtual currencies entered into force on March 10, 2020. Among the services that require an operating licence, exchanging a virtual currency for a virtual currency was added, different VC services were united under the umbrella term of providing a service of virtual currency. With the amendment the requirements for providing the service were made considerably more strict, including the requirement that a prerequisite for possessing an operating licence is that the actual location of business activities is Estonia. The duties of due diligence have also been made more severe. Whereas previously it was not obligatory for the service providers to identify customers if as occasional transaction was of less value than 15,000 euros, now the customer must be identified in any case. In addition to that, stricter rules entered into force for checking the identity of citizens of third countries. The entrepreneurs who had already a VC operating licence became obliged to harmonize their activity with the law amendment by July 1, 2020. The law amendments have made it possible for the *RAB* to order the market considerably. During the period of 01.03.–31.08.2020, the *RAB* declared in total 1296 VC operating licences null and void (licences for the service of exchanging VC for money as well as licences for the wallet service; most of the enterprises had both of the licences).

The third chapter of the inquiry, that concentrates on the crime risks of the sector, allows to conclude that, despite the law amendment mentioned, the risks around the VC sector are very high and it is likely that the level of due diligence of enterprises does not rise sharply. Because of that, the VC branch should receive continuously extra attention in the framework of proceedings of operating licences and supervision as well as from investigation institutions and the legislator. The regulation concerning the VC sector should further be made more strict. An obligation for VC enterprises should be introduced to report at least about the customers and the turnover of the transactions mediated. In addition to that, supplementary measures should be taken to protect persons and their assets, which would also include requirements for information systems, cybersecurity and data handling.

In the sphere of prevention and investigation of crimes connected to virtual currencies more emphasis should be laid on international cooperation because almost all of the cases have an international scope and it is time-consuming to gather the necessary information. The cooperation is not efficient with many countries; that makes it even more complicated to discover the schemes and to prevent crimes in the area of VC.