Public Governance, Administration and Finances Law Review Vol. 5. No. 1. (2020) • 38–47.
10.53116/pgaflr.2020.1.2

European Legal Regulation of Cryptocurrencies through the AML Scope

Pavel Datinský*

* Pavel Datinský, M.A. in Law, PhD candidate at the Department of Financial Law, Faculty of Law, Masaryk University in Brno, the Czech Republic, email: felifox@seznam.cz, ORCID: https://orcid.org/0000-0002-0495-0439

Abstract: This article deals with cryptocurrencies and its impact nowadays on the AML field at a European Union level. The article will be divided into an introduction, four chapters and a conclusion; it will define elementary information and defitions, will identify ways of practical use of cryptocurrencies, will introduce risks connected with the use of cryptocurrencies and will introduce legal regulation of cryptocurrencies by the V. AML Direction. In the conclusion the quality of communitary regulation will be evaluated and a few *de lege ferenda* tips will be devised to improve regulation for the future.

Keywords: cryptocurrencies, Bitcoin, anti money laundering, European Union, regulation

1. Introduction

Cryptocurrency is a phenomenon of the last decade which attracts the attention of all legal and economic professionals and the non-professional public. Since 2009, when the mysterious creator Satoshi Nakamoto launched the system of Bitcoin, the amount of cryptocurrencies is steadily growing. There were around 3,200 (www.coinlore.com) known cryptocurrencies at the beginning of 2020 and there were an estimated 2.9–5.8 million of active cryptocurrency "wallets" at the end of 2017 (Hilleman & Rauchs, 2017). Although cryptocurrencies used by general public, which served as an inspiration for this article, form only a fraction of this amount. Bitcoin serves as a basis for this article, since it is the oldest and probably the most well-known cryptocurrency, and thanks to many years of tradition, it is possible to excellently demonstrate the evolution of its value and other contextual qualities.

In this article I will first define the term cryptocurrency and the term virtual currency – which is semantically superior to the term cryptocurrency – and then I will demonstrate several ways in which cryptocurrencies are most used nowadays. Subsequently, I will demonstrate the risks associated with the use of cryptocurrencies, based on my earlier publications (Datinský 2018a; Datinský 2018b), but in this article, unlike in the previous works, I will focus on the public risks that occur throughout the European Union. From the public law risks associated with the use of cryptocurrencies, I will focus more on the area of money laundering and the financing of illegal transactions, including specific cases of using cryptocurrencies for illegal transactions. In the final part of this work I will evaluate the current Community legislation of the field and its effectiveness in relation to combating money laundering and financing of illegal transactions.

2. Literature overview

Expert papers and opinions of expert institutions of the European Union were used to compose this paper in order to substitute missing legal or communitary definitions and to explain the functions of cryptocurrencies. Communitary and Czech regulations were used further in this paper to demonstrate the relevant regulation of the subject matter. Specialised websites are cited in order to demonstrate recent trends and technical options in the scope of cryptocurrencies, too. Finally, expert monographies about the subject matter of this paper were used and cited in this paper.

3. Research

An analysis of basic concepts and functions were performed in this paper. Comparative method was used for a comparison of two elementary kinds of currencies (crypto and fiat) and analytic method was used for the demonstration of elementary functions and consequences of these two kinds. The inductive method was used to introduce special risks related to the use of cryptocurrencies, and finally, simple steps were deduced, capable of eliminating the presented risks. The research methods used in this paper were analysis, comparison, induction and deduction.

3.1. What is cryptocurrency?

Before defining the very term cryptocurrency, it is appropriate to define the term superior to cryptocurrency, namely, virtual currency, of which the cryptocurrency is a subset. The specific legislative definition of virtual currency has been absent for quite a long time in European law, and this concept has been defined by European professional institutions, but in a rather negative way, i.e. by defining what these virtual currencies are not. The European Banking Authority defined the virtual currency as *"a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a FC, but is used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically"* (EBA, 2014, 11). Financial Action Task Force defined the virtual currency in a very similar way as a *"digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency"* (FATF, 2014, 4). Some time later the European Central Bank has adopted a document in which it defined the virtual currency as *"a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money"* (ECB, 2015, 33).

With the increasing interest in the use of virtual currencies by the general public for a variety of purposes, which I will mention below, the need for national and Community legislators to regulate this phenomenon has increased in proportion. At national level,

some Member States have made at least partial regulatory efforts.[1] At Community level, however, a significant shift in the approach to and regulation of virtual currencies occurred only with the adoption of Directive 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 financial system for purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, or so-called "V. AML Directive" (hereinafter referred to as "The V. AML Directive").

This directive now contains a specific legislative definition of the term virtual currency, defining it this way: "a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically" (V. AML Directive, Article I, paragraph 2, letter d, no. 18).

It is therefore possible to deduce the basic conceptual characteristic of virtual currency from the above mentioned definitions, which is independence from the public authority of any state, whether related to the issuance of virtual currency or its circulation among users.

Virtual currencies can then be categorised according to whether they are issued by one or by a specific, narrower group of their users (centralised) or by an unspecified number, or more precisely by all its users (decentralised) and whether or not they are generally exchangeable among their users. Bitcoin, for example, which serves as a basis for this article, is a typical decentralised and exchangeable virtual currency. In the category of virtual currency centralised and unexchangeable, there can be a variety of values or currencies used in computer and mobile games, which players can buy or otherwise acquire in the game, and for which they can then buy various virtual items or services associated with the game itself.

This implies that typical cryptocurrencies are decentralised virtual currencies, as they are generally issued by all or an unspecified number of users (miners) without the interference of any authority. Since these virtual currencies are specifically encrypted by so-called cryptography to be readable and usable only by their users, the term cryptocurrency was derived from this method of encryption. The technical methods of origin and encryption, and technical aspects of cryptocurrency usage will not be dealt with in this work, as it would go far beyond its limited scope and other, technically more knowledgeable authors publish regularly on this matter (Lánský, 2018; Biryukov et al., 2014).

Through the optics of the legal order of the Czech Republic, the cryptocurrency unit can be described as a thing within the meaning of Act No. 89/2012 Coll., The Civil Code, as amended, namely a movable, intangible thing. A similar categorisation of the cryptocurrency unit can with high probability be performed under other European national legal systems. As with classic money, or more precisely banknotes, the subject of discussion might be whether or not is the cryptocurrency fungible. For payment system participants

[1] For example in the Czech Republic the national legislator specified by way of a general clause which subjects are liable to AML obligations and which subjects provide services connected to the virtual currencies; see Section 2, paragraph 1, letter l) of Act. No. 253/2008 Sb., on selected measures against legitimisation of proceeds of crime and financing of terrorism.

aiming at transferring the value of a unit from one entity to another, it will be considered fungible, but each cryptocurrency unit is represented by a specific program code that makes it unique, just as each banknote has its own unique serial number, different from all others, and therefore might be considered irreplaceable for a certain group of public.[2] Through the investor's optics a cryptocurrency unit may be viewed as a commodity and is also usually traded in the same way (Hampl, 2014).

3.2. Ways of using cryptocurrencies

Despite the fact that, according to the above mentioned definitions, cryptocurrencies are not legal tender, they are used very frequently for payment. The indisputable advantage of using cryptocurrency as a payment instrument is its minimal near-zero transaction costs and the considerable rate of transfer of its units among its users, not limited by geographical or political boundaries, which constitutes a significant advantage over foreign payments through standard payment service providers. To some extent, the anonymity of cryptocurrency users, who are almost entirely anonymous until the potential exchange of the cryptocurrency for a legal currency, may be considered an advantage, as they are only one member of a large, unspecified group of cryptocurrency users. The reverse side of the coin of these benefits is that cryptocurrencies are a very handy means of financing illegal transactions, terrorism, and can be used to legalise the proceeds of crime, as I will mention below.

As the demand for cryptocurrencies continues to grow and new types are constantly appearing, this high demand logically pushes up the price at which cryptocurrency units can be purchased. This has resulted in considerable interest in cryptocurrencies by speculators and investors who hope that the units they buy will grow in value over time, which often happens.[3] The first collective investment funds, focused on cryptocurrencies, start to operate nowadays. The first similar fund in Central Europe is a fund established by a Czech management company, called the Kryptofond (a typical name), and managed by CFG Funds s.r. o.[4] It was opened on January 31, 2018, but in the form of a private fund for qualified investors, managed by its management company pursuant to Section 15 of Act No. 240/2013 Coll., based on Article 3 of the European Parliament and Council Directive No. 2011/61/EU (AIFMD Directive), under a regime not subject to supervision by the national supervisory authority. In addition to the European cryptofund, there are a number of similar funds, the largest of which are based in the United States of America, and are managed by Grayscale Investments, LLC,[5] which focus more on individual cryptocurrencies and are not very diversified. However, these non-European funds are also special funds intended for qualified, private investors and are not publicly offered.

[2] I.e. collector's banknotes, or the very first Bitcoin code, the so-called Genesis block.
[3] See www.kurzy.cz
[4] See www.kryptofond.cz
[5] See www.grayscale.co

3.3. Risks associated with the use of cryptocurrencies

The aforementioned uses of cryptocurrencies as tools for paying or investing involve a number of risks that endanger not only the users themselves, but also the wider public. For the purposes of this work, these risks could be categorised into (i) private-law risks, i.e. those that endanger cryptocurrency users themselves, without overlapping into the general public, and (ii) public-law risks, that endanger society as a whole, nonetheless it is clear that private-law risks will extend to the public sector and, if they occur more frequently, endanger the wider public. Likewise, the manifestation of public-law risks will also have an impact on the users themselves.

I have dealt with the private-law risks in my earlier publications cited at the beginning of this article, so here I will focus on public-law risks with a transnational outlook; due to lack of geographical limitations of cryptocurrency use, these risks objectively threaten the whole, not only European, society.

Public-law risks usually fulfil the actus reus of some typical crimes against the currency and payment system of individual Member States, which, thanks to the single currency of the European Union, have a Community dimension. A typical case may be the occurrence of entrepreneurs offering their goods or services within the EU and requesting that their goods or services be paid exclusively by cryptocurrency, which may put the entire financial system at risk, although this is not yet the case on a larger scale.

With the growing volume of money exchanged for cryptocurrencies, the risks related to tax law also increase, as due to the anonymity of users, they do not have to voluntarily declare their profits on cryptocurrency investments, which in some cases can be quite substantial. The national tax authorities then do not have the possibility to check online wallets of cryptocurrency users in any way and are not able to find out by their control activity whether or not the given cryptocurrency user made an investment profit. However, the tax issue will not be discussed in this work.

A significantly more dangerous public-law risk is the relatively easy possibility of legalising the proceeds of crime, conducting illegal transactions and financing terrorism, which is very difficult to detect due to anonymity of cryptocurrency users and the above mentioned cryptocurrency decentralisation; the anonymity of the specific cryptocurrency issuer is also very difficult to regulate.

Socially the most widespread cryptocurrency, Bitcoin, allows all its users to transfer unlimited Bitcoin units, which in fact means making payments for any goods or service between those users. However, due to the above mentioned anonymity of their users, it is not traceable for what the payment was made or to whom it was addressed, as opposed to normal payments using the common currency, the so-called "fiat" currency, and related banking services. This risk has long been perceived both at the level of individual Member States (e.g. Methodological instruction No. 2 of the Financial Analytic Entity of the Ministry of Finance of the Czech Republic) and, over time, at EU (V. AML Directive preamble, Article 8,9) and international (IMF, 2016, p. 24) level.

A typical example of illegal cryptocurrency transactions is the purchase of illegal goods (drugs, weapons, etc.) in the so-called Dark Web Markets such as Silkroad, which actually operates as an e-shop, even with individual vendor ratings by the users of this

"e-shop" themselves, where the visitor chooses the appropriate goods, filters out the ideal supplier with the most favorable rating and price, and then pays for that order in cryptocurrency. Regardless of whether the outgoing payment goes to a risk country in terms of Article 9 of the V. AML Directive or whether its quantity exceeds the limits requiring client check or enhanced client check, the payment is made anonymously, immediately and the seller sends the order to the agreed address. This also benefits some terrorist groups, which finance their activities by these means and buy weapons for their attacks (Whyte, 2019, p. 10–11).

The above mentioned abuse of cryptocurrencies for illegal purposes is not easy to combat and regulate. As mentioned previously in this article, the absence of a specific issuer makes it impossible to supervise and in any way regulate the issue of cryptocurrency, or more precisely the actual creation of their units. In the absence of this subject, the question arises as to what other subjects in the cryptocurrency system are involved and whether these subjects can be effectively targeted with appropriate behavioral rules. These persons are then:

(i) cryptocurrency users themselves,
(ii) cryptocurrency miners, i.e. persons who actually create cryptocurrency units with their hardware, without having to buy them at the relevant cryptocurrency exchange offices,
(iii) so-called digital wallet providers that allow cryptocurrency units to be stored by individual users,
(iv) developers,
(v) persons who initiate first offer of the cryptocurrency, so-called Initial Coin Offering (ICO), which is equivalent to IPO (Initial Public Offering) in the case of an initial issue of securities on a stock exchange,
(vi) cryptocurrency exchange offices that allow the exchange of individual types of cryptocurrencies with one another, or the exchange of a fiat currency with a cryptocurrency,
(vii) cryptocurrency exchanges where individual cryptocurrencies are traded in the form of centralised and decentralised exchanges.

Cryptocurrency users are anonymous within the system, so it is difficult to control them technically. Miners are only a subset of cryptocurrency users, so even those are not easy to regulate. Developers are IT professionals who develop and program new cryptocurrency systems, therefore their regulation is not desirable, at least at a time when the use or creation of cryptocurrencies is generally not prohibited. ICO initiators, like developers, are not persons who would actively participate in the use of cryptocurrencies as users, but only those who receive funding for developing new or improving existing cryptocurrencies, thus regulating this activity would not again address the above outlined problems with the legalisation of proceeds or the execution of illegal transactions. On the other hand, these are entities who come into contact with future users who want to exchange their fiat currency for a new cryptocurrency, so they could be considered in an analogous way to those who provide currency exchange activities that I will mention below. It might seem logical to regulate cryptocurrency exchanges where cryptocurrencies and fiat currencies are

exchanged, but when they occur in decentralised form, it is only by way of a programmed software without a particular owner or operator, to whom specific obligations could be imposed. Regulation could therefore only affect centralised exchanges, subject to management and organisation by a specific person. It might seem logical to regulate the provider of virtual wallets, but as of 9 January 2020,[6] no identification data of its owner was needed for the creation and use of such a wallet, as is the case when opening a common bank account for fiat currency (Pytlík, 2019, p. 65–67).

From all of the above, it seems the easiest to regulate the cryptocurrency exchange offices, in which real fiat currencies are exchanged for digital currencies and vice versa, since these entities allow a person to enter the cryptocurrency system. When purchasing cryptocurrency units or exchanging them for a fiat currency, it is possible, and according to the author also desirable, to carry out an appropriate check of the client (the person performing the exchange) within the scope of AML. At the same time, an important fact is that the elementary objective of any person legitimising the proceeds of crime is to obtain some real return in the form of fiat currency, property or other benefits at the end of the legalisation process, whereas according to the author cryptocurrencies do not constitute a real return yet, therefore, one must use a virtual exchange office to achieve this.

On the other hand, even the regulation of currency exchange offices and client checks when entering or exiting the system may not solve the problems outlined above and eliminate the risks of illegal use of cryptocurrencies, as the originally exchanged fiat currency may come from purely legal sources and cryptocurrencies purchased for it may then serve for financing illegal transactions. Conversely, the true origin of the cryptocurrency, which is exchanged for fiat currency, may be debugged by the user and the exchange office does not have the means to verify such information in any way. In conclusion of this part of this article, it is worth mentioning that the anonymity of cryptocurrency users in the execution of transactions is not in all cases boundless. The European Union finances and operates the so-called Titanium Project,[7] which is exploring new ways and tools that can be used to deanonymise cryptocurrency transactions for the purpose of investigating crimes, and this project has seen partial success with, for example, the Bitcoin cryptocurrency. However, the whole process is very complex and costly, and is not yet used on a larger scale.

3.4. Cryptocurrency regulation within the scope of the V. AML Directive

The author's above mentioned opinion on the necessity of regulation of exchange offices providers corresponds with the current Community legal regulation of AML, implemented by the V. AML Directive, Article 8, where the need to include persons carrying out currency exchange activities and persons providing virtual wallet services among the liable entities within the meaning the AML is explcitely stated. In Article 9, the Directive then identifies

[6] A New AML Directive enters into force on 10 October 2020 and includes these providers as entities liable to AML obligations, as specified below.

[7] See www.titanium-project.eu

the anonymity of cryptocurrency users as a reason for its potential misuse for the purpose of crime, which also corresponds to the above mentioned opinion of the author.

The V. AML Directive is to be seen as the first significant and highly anticipated step by the EU legislator towards effective regulation of cryptocurrency transactions and prevention of their use for illegal transactions, although it is rather a small step towards comprehensive regulation of this area. Below are listed some of the major innovations that the V. AML Directive has brought.

The basic benefit is the embodiment of legal definition of virtual currency in Article 3 of the V. AML Directive, which has so far been defined only by individual professional institutions; furthermore, the definition of a virtual wallet provider, which is newly considered a liable entity under the AML Directive, and finally the classification of a currency exchange provider between virtual currencies and fiat currencies as liable entity. The above is also related to the extended method of performing the in-depth check of the client according to Article 13, which also allows the inspection to be carried out in accordance with *"electronic identification means, relevant trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council or any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities"*, which can greatly speed up the client's in-depth check, for example by using client data from his/her personal bank, whose card, for example, carries out transactions and purchases cryptocurrency units.

According to Article I (29) of the V. AML Directive, the above mentioned new liable entities are then subject to registration with the competent AML authorities, furthermore, exchange offices will even be subject to authorisation procedures, which should ensure faster and more transparent control of transactions provided by these entities, and should also ensure obligatory qualification of persons providing such services.

The resulting effect is that if a person exchanges a fiat currency for a cryptocurrency within the EU, the V. AML Directive requires that the exchange service provider, listed with the supervising AML authority, is obliged to check and identify the client. Since very often a virtual wallet service is offered along with an exchange for cryptocurrency to a customer, especially for new cryptocurrency users who are not yet using such wallet, the wallet and its public key are then identifiable and associated with the particular cryptocurrency user identified during the exchange upon receipt/assignment of the virtual wallet by the liable person (exchange office).

The resulting situation after the adoption of the V. AML Directive thus by far does not comprehensively address the question of the misuse of cryptocurrencies for illegal transactions from the perspective of AML, as the transparency of cryptocurrency transactions and the identification of persons carrying out transactions is still not ensured, although this is not due to lack of effort of Community legislators, but mainly to nowadays' technical possibilities. It is a question of the future whether technologies for deanonymising cryptocurrency transactions, decentralised cryptocurrency exchanges, and similar means that serve cryptocurrency users and facilitate their illegal transactions, will be developed more effectively and faster. According to the author, the current EU regulation, with regard to the current technical possibilities, is appropriate and can be described

as rather good. The author considers the exclusion of persons operating centralised electronic cryptocurrency exchanges as liable entities as a minor deficiency of the new regulation.

4. Conclusion

In the presented work, the basic notions of the examined material were defined, namely the the terms virtual currency, cryptocurrency and the most common uses of cryptocurrencies. The risks associated with the use of cryptocurrency as a means of payment were also identified and the possibility of misuse of cryptocurrencies to legalise the proceeds of crime and finance illegal transactions was identified as a major risk. The existence of this risk is mainly due to the anonymity of cryptocurrency users and individual transactions, as well as the absence of an entity that could be subject to effective regulation, that is a regulation that would prevent specific ways of misusing cryptocurrency payments. Currently, the only entities that can be effectively regulated are virtual exchange service providers, where cryptocurrency is exchanged for fiat currency, and virtual wallet providers, that allow users to securely make payments with their cryptocurrency.

These entities are therefore targeted by the current European AML legislation, embodied in the V. AML Directive, which included these entities as liable entities within the meaning of the AML, therefore if, after the Directive enters into force in the EU, a person will exchange fiat currency for cryptocurrency and will be assigned a virtual wallet, providers of such services will be obliged to check the client and identify him/her. With this adjustment, virtual wallet owners who participate in selected virtual payments will be identified and will lose their anonymity. Likewise, when someone exchanges a fiat currency for a virtual currency, he will be subject to obligatory identification or check under the AML rules.

These benefits of the V. AML Directive do not, of course, fully address the issue, but with regard to the current technical possibilities, more precisely the impossibility of disclosing the anonymity of cryptocurrency users, the current legal regulation may be considered appropriate. A minor drawback may be the exclusion of centralised virtual exchanges operators among liable entities.

References

Biryukov, A., Khovratovich, D., & Pustogarov, I. (2014). Deanonymisation of clients in Bitcoin P2P Network. Ithaca: Cornell University press,. https://arxiv.org/abs/1405.7418 https://doi.org/10.1145/2660267.2660379

Datinský, P. (2018a). Fondové investování do kryptoměn [Fundinvesting into Cryptocurrencies] [Paper presentation]. COFOLA international conference, section II, Peníze, měna a právo (Money, monetary, law).

Datinský, P. (2018b). K právní regulaci kryptoměn [Legal regulation of Cryptocurrencies] [Paper presentation]. International on-line conference QUAERRE.

EBA (2014). EBA Opinion on 'virtual currencies'. European Banking Authority. https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1

ECB (2015). Virtual currency schemes – a further analysis. European Central Bank. www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

FATF (2014). Virtual Currencies Key Definitions and Potential AML/CTF Risks. FATF Report. www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Hampl, M. (2014). Víceguvernér ČNB „vrací úder" aneb polemika kolem bitcoinů pokračuje [The Vice Governor of the Czech National Bank "strikes back" or the polemic about Bitcoins keeps going]. Roklen 24. https://roklen24.cz/a/iTznt/viceguverner-cnb-vraci-uder-aneb-polemika-kolem-bitcoinu-pokracuje

Hileman, G. & Rauchs, M. (2017). Global Cryptocurrency benchmark study. Cambridge: University of Cambridge. www.crowdfundinsider.com/wp-content/uploads/2017/04/Global-Cryptocurrency-Benchmarking-Study.pdf https://doi.org/10.2139/ssrn.2965436

IMF (2016). Virtual Currencies and Beyond: Initial Considerations. IMF Staff Discussion Note. www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf

Lánský, J. (2018). Cryptocurrencies (1. version). C. H. Beck.

Pytlík, R. (2019). Kryptoměny – dopady v oblasti AML [Cryptocurrencies – impacts in the AML field] [Thesis]. Brno, Masaryk University, Faculty of Law. https://is.muni.cz/th/tgjaa/

Whyte, Ch. (2019). Cryptoterrorism: Assesing the utility of blockchain technologies for the terrorist enterprise. Studies in Conflict & Terrorism. Taylor and Francis Online. www.tandfonline.com/doi/abs/10.1080/1057610X.2018.1531565?journalCode=uter20 https://doi.org/10.1080/1057610X.2018.1531565

Legal sources

EU laws

- 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;
- Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC;
- Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010.

Czech Republic laws

- Act No. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, as amended;
- Act No. 89/2012 Sb., občanský zákoník, as amended;
- Act No. 240/2013 Sb., o investičních společnostech a investičních fondech, as amended.
- Methodological instruction No. 2 of the Financial Analytic Entity of the Ministry of Finance of the Czech Republic, from 16 September 2013, designed for obliged entities, about the approach of the obliged entities for virtual currencies. www.financnianalytickyurad.cz/download/FileUploadComponent-1133285150/1506340773_cs_1481699516_cs_2-pokyn-mf_c-002_2013-09_metodicky-pokyn-o-pristupu-povinnych-osob-k-digitalnim-menam.pdf