

All that Glitters is not Gold: The Regulation of Virtual Currencies in the New EU V Anti-Money Laundering Directive

di Sara De Vido

Abstract: Non tutto quello che luccica è oro: la regolazione delle montete virtuali nella V direttiva contro il riciclaggio – The purpose of this article is to provide a first comment to the new provisions on virtual currencies included in the European Union Directive 2018/843, amending Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, known as Fifth Anti-Money Laundering Directive. The Directive requires States to include, among the obliged entities to respect anti-money laundering and counter-terrorism financing requirements, such as ‘know-your-customer’, the ‘providers engaged in exchange services between virtual currencies and fiat currencies.’ To the big dilemma: ‘to regulate or not to regulate’ virtual currencies, including Bitcoins, the EU answered that yes, we must regulate. However, what is the meaning of regulating Bitcoins? After presenting what VC are and which challenges they pose to international law, I will argue that regulation is fundamental in order to avoid the exploitation of these currencies for the purposes of money laundering and terrorism financing, but that, at the same time, regulation as it was conceived at EU level might pose numerous challenges because it only concerns the moment in which the ‘real’ world meets the ‘virtual’ one, and is applicable only to the obliged entities that fall under the scope of the EU legal instrument.

59

Keywords: Cryptocurrencies; Anti-Money Laundering; Bitcoin; EU law.

1. Introduzione

The purpose of this article is to provide a first comment to the new provisions on virtual currencies included in the European Union (EU) Directive 2018/843, amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, known as Fifth Anti-Money Laundering Directive (V AML Directive), approved by the European Parliament on 19 April 2018, and published in the Official Journal of the EU on 21 June 2018.¹ The Directive requires States to include, among the obliged entities to respect anti-money laundering (AML) and counter-terrorism financing (CFT) requirements, such as ‘know-your-customer’, the ‘providers engaged in exchange services between virtual currencies and fiat currencies.’ To the big dilemma: ‘to regulate or not to regulate’ virtual currencies (VC), including

¹ Directive (EU) 2018/843 of the European Parliament and 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 and terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, *GUL*-156/43, 19.06.2018.

Bitcoins, probably the most famous one currently existing in the world, the EU answered that yes, we must regulate. However, what is the meaning of regulating Bitcoins? I will argue that regulation is fundamental in order to avoid the exploitation of these currencies for the purposes of money laundering and terrorism financing, but that, at the same time, regulation might pose numerous challenges because it only concerns the moment in which the ‘real’ world meets the ‘virtual’ one, and is applicable only to the obliged entities that fall under the scope of the EU legal instrument.

The article will first present the world of virtual currencies, stressing the challenges they pose to international law, and will explore risks and vulnerabilities of these currencies to money laundering and terrorism financing. I will then delve into the new V AML Directive, explaining why an amendment to the previous IV AML Directive was long-awaited to include virtual currencies within the scope of application of the Directive. I will eventually reflect on the legal implications of the regulation, and its related and unresolved issues.

2. Virtual currencies

60

‘What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.’² The idea of Nakamoto, name that surely identifies a/several pseudonymous software developer(s), was to create a system based on cryptography to replace the traditional banking system, which, after the outburst of the financial crisis back in 2008, was considered not as reliable as it was in the past, if ever was. To put it simply, maths and trust among peers, instead of trust to the traditional centralised financial system. After ten years, Bitcoins still exist, and have recently gained much more attention. At the beginning of 2018, economists and financial experts warned against the Bitcoins’ ‘bubble,’ which was compared to, and considered more severe than, the tulips’ bubble in 1630s. In a study reported by Bloomberg in April 2018, a team of the Bank of America Corporation defined Bitcoins as ‘the greatest bubble in history.’³ Coindesk later replied to the study saying that, due to the trend of Bitcoins over the years, the analysis was not fair.⁴ It should be acknowledged indeed, as two authors said, that ‘the death of Bitcoin’ has been announced more than one hundred times since its creation, but it has never happened, and ‘Bitcoin increasingly is being integrated into the governance of mainstream monetary systems.’⁵

Since the purpose of our analysis is purely legal, we will not delve further into economic considerations, which would be however interesting, because stability and reliability are key factors in convincing people to buy, use, invest with one currency rather than with another. We will see however that in the case of

² S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, 1, www.bitcoin.org (last access to all websites 1. March 2019).

³ www.bloomberg.com/news/articles/2018-04-09/bitcoin-seen-popping-like-the-greatest-bubbles-by-bofa

⁴ www.coindesk.com/bank-of-america-bitcoin-bubble-is-already-popping/ (last accessed on 21 June 2018).

⁵ M. Hütten, M. Thiemann, *Moneys at the margins. From political experiment to cashless societies*, in M. Campbell-Verduyn, *Bitcoin and Beyond Cryptocurrencies, Blockchains, and Global Governance*, Abingdon, 2018, 25.

Bitcoins, what is appealing is its (although partial) anonymity, which might be exploited by criminals to hide illicit activities.

We will first start from a definition of VC, and of Bitcoins more specifically, trying to trace the origins and the evolution of these currencies.

2.1. Definitions and characteristics of VC, with specific regard to Bitcoins

According to the Financial Action Task Force on Money Laundering, an international body established in 1989 by the then G7 to tackle the problem of money laundering, in its report of 2014:

Virtual currency is 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 (i.e., when tendered to a creditor, is a valid and legal offer of payment) 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.⁶

VC must be distinguished from fiat currency, meaning coins and paper money of a country that is designated as its legal tender, and from e-money, which consists of a digital transfer mechanism for fiat currency. VC can be either convertible or non-convertible. The former can be exchanged for fiat currency at any time; the latter are created and exploited in the virtual world only.⁷ Scholars have extensively discussed on the nature of VC as money.⁸ This debate will not be covered in this contribution, which will only take into account the position adopted by the EU in that respect.

VC can also be centralised, meaning that there is a third party that controls the system, and establishes rules at the same time. To the contrary, decentralised virtual currencies, also called crypto-currencies, are ‘open-source, math-based peer-to-peer virtual currencies that have no central administrating authority, and no central monitoring or oversight.’⁹

The origin of virtual currencies dates back to the 1980s. It was a researcher, David Chaum, who first used cryptographically signed tokens which represented a fixed amount of money.¹⁰ He first invented in 1984 an untraceable payment system based on blind signatures, and then in 1990 he refined his creation by putting it online: that is how e-cash started, promoting anonymity, which will

⁶ FATF, *Virtual Currencies. Key Definitions and Potential AML/CTF Risks*, June 2014, 4.

⁷ Ivi, 4.

⁸ See, for example, just to name a few, S.A. Wolla, *Bitcoin: Money or financial investment?*, Federal Reserve Bank of St. Louis, March 2018, research.stlouisfed.org, who considers that Bitcoins lack some of the requirements to be considered as ‘currency’; S. Lo, J.C. Wang, *Bitcoin as money?*, 2014, www.bostonfed.org/publications/current-policy-perspectives/2014/bitcoin-as-money.aspx, on how Bitcoins fulfilled the functions of a fiat money; S. Capaccioli, *Criptovalute e bitcoin: un’analisi giuridica*, Milano, 2015, 114, who considers it as ‘a new form of currency’; O. Lakomski-Laguerre, L. Desmedt, *L’alternative monétaire Bitcoin: une perspective institutionnaliste*, in *Revue de la régulation*, 18, 2015, online journals.openedition.org/regulation/11489, focusing on ‘la capacité du projet Bitcoin à construire un ordre monétaire, certes alternatif, mais stable.’

⁹ Ivi, p. 5.

¹⁰ J. Baron, A. O’Mahony, D. Manheim, C. Dion-Schwars, *National Security Implications of Virtual Currencies*, Santa Monica, 2015, 10.

become the pivotal feature for future currencies.¹¹ It was not the proper origin of VC as they are conceived today, though.

By the end of the century, computational systems allowed the creation of money. Hence, for example, in 1998, ‘b-money’ and ‘bit gold’ represented money created through the solution of computationally difficult problems, the amount of money being proportionate to the degree of difficulty of the problem.¹² The year after, two researchers introduced an anonymous electronic cash system which did not require a central server, where a coin was represented by the hash of its serial number.¹³

Compared to the first attempts of VC, Bitcoins was different because of its decentralisation. As reported in the website Coindesk, Bitcoin is the word that both identifies the token - ‘a snippet of code that represents ownership of a digital concept,’ - and the protocol, ‘a distributed network that maintains a ledger of balances of bitcoin-the-token.’¹⁴ Payments are allowed between the users without passing through a central authority, such as a bank, or another financial institution. No authorisation of any sort is required.¹⁵ Compared to other fiat currencies, Bitcoins are of limited supply. The maximum amount of Bitcoins was set since its inception at 21 million.¹⁶ Since the process of ‘mining’¹⁷ Bitcoins is at a slower pace year after year, and the costs in terms of software are higher and higher, the maximum is scheduled to be reached in more than one century. Anyone can download a free software from the website to send, receive and store Bitcoins. The procedure can be clearly explained as follows:

When the client is initially run, the application generates a set of cryptographic keys that are mathematically related to one another. One key is private and remains concealed on the user’s computer. The other key, often referred to as a Bitcoin address, is made public; it is used to accept Bitcoin payments from other users. Together, these keys serve as the user’s digital signature.¹⁸

Bitcoin addresses have the same function as an account. All transactions are gathered in a publicly available transaction register, which is identified by the Bitcoin address, a string of letters and numbers. Copies of transaction records (ledgers) are kept in multiple computers in the network and visible to anyone.¹⁹ A network of computing ‘nodes’ constitutes the ‘blockchain,’ which is the underlying technology behind Bitcoins. The blockchain ‘records the path of every Bitcoin as it changes hands through the network, thereby functioning as the definitive public

¹¹ P. Franco, *Understanding Bitcoins, Cryptography, Engineering and Economics*, John Wiley & Sons, Chichester, 2014, 162-163.

¹² Ivi, 164.

¹³ Ibid.

¹⁴ www.coindesk.com/information/what-is-bitcoin/.

¹⁵ R. Böhme, N. Christin, B. Edelman, T. Moore, *Bitcoin: Economics, Technology, and Governance*, in *Journal of Economic Perspectives*, 29, 2015, 214.

¹⁶ coinmarketcap.com/currencies/bitcoin/ 17.590.025 BTC have already been mined.

¹⁷ A miner can be both a natural or legal person that creates Bitcoins by using a software. A person can generate Bitcoins for his/her own purpose, or can participate in a virtual currency system as exchangers. It is a software that produces Bitcoins. The higher the number of Bitcoins, the more difficult the process to mine Bitcoins.

¹⁸ J. J. Doguet, *The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System*, in *Louisiana Law Review*, 73, 2013, 1126.

¹⁹ IMF, *Virtual Currencies and Beyond: Initial Considerations*, www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf, 20.

ledger of every user's account balance.'²⁰ Blockchains are 'digital sequences of numbers coded into computer software that permit the secure exchange, recording, and broadcasting of transactions between individual users operating anywhere in the world with Internet access.'²¹ Transactions are confirmed and checked by the users themselves, creating a system that, at least in principle, is extremely reliable. In principle, indeed, more than in reality. The reason is that even though private keys are encrypted, and a password is needed to read them, it is also true that passwords are often too easy to identify, either being excessively weak (as the majority of people tend to do), or because they are cracked. Bitcoins are considered to be 'pseudo-anonymous,' which means that the user does not need to identify him/herself before sending Bitcoins, and the protocol will only be checked when the sender has the amount of Bitcoins necessary to conclude the transaction.

2.2. How they work

Even though the blockchain technology seems complex, everyone can buy Bitcoins and use them. The steps to obtain Bitcoins are indeed – not surprisingly – easy. Not surprisingly because the purpose of this currency has been, since the very beginning, to 'democratise' the financial system, through a mechanism of access which was conceived as being easy and devoid of costs. Every step is clearly explained on the web.²² You first set up a wallet, which necessary to store your Bitcoins, and this can be an online, desktop, mobile or offline wallet. Every wallet is identified through a string of characters and/or passwords. Then you need a cryptocurrency exchange to buy and sell Bitcoins. It is immediately clear that the absence of intermediaries that was at the basis of the system is not technically respected. It is respected when it comes to payments, but not at the moment in which the virtual world meets the real one. Two authors have not considered bitcoins as a means of exchange, but rather as 'a form of game played in a society,' which, though being innovative and born to be 'anti-statist' and 'anti-establishment', has been facing a phase of 'normalisation,' meaning of integration in the financial system.²³ As we will see in the forthcoming paragraphs, VC exchange providers are considered as all other financial institutions for the purposes of anti-money laundering and counter-terrorism financing, and hence they have become part of the financial system. In the website Coindesk, users are informed that '[w]ith the clampdown on know-your-client and anti-money-laundering regulation, many exchanges now require verified identification for account setup. This will usually include a photo of your official ID, and sometimes also a proof of address.'²⁴

Once the exchange receives the payment, it will purchase the corresponding amount of Bitcoins to be deposited in an automatically generated wallet. Then, Bitcoins can be transferred to an off-exchange wallet. Bitcoins can also be bought with cash using ATMs.²⁵

²⁰ J. Doguet, *The Nature of the Form, cit.*, 1126.

²¹ M. Campbell-Verduyn, *Introduction*, in M. Campbell-Verduyn, *op.cit.*, 1.

²² www.coindesk.com/information/how-can-i-buy-bitcoins/

²³ Hütten, Thiemann, *op. cit.*, 25.

²⁴ www.coindesk.com/information/how-can-i-buy-bitcoins/

²⁵ In Italy there are 31 ATMs that are able to convert cash into bitcoins according to the website coinatmradar.com/country/105/bitcoin-atm-italy/

2.3. *Pros and cons of virtual currencies: All that glitters is not gold*

Despite being highly criticised for the reasons we are going to explain in this paragraph, the potential of these currencies, or better, of the technology backing these currencies, is enormous, as confirmed by Christine Lagarde, the Managing Director of the International Monetary Fund, in a recent IMF blog:²⁶

The technology behind these assets - including blockchain - is an exciting advancement that could help revolutionize fields beyond finance. It could, for example, power financial inclusion by providing new, low-cost payment methods to those who lack bank accounts and in the process empower millions in low-income countries.

The technology that was developed for Bitcoins – blockchain – can be used for other purposes. Fintech, the financial technology, seems to be only at a first stage, indeed.²⁷ The system is based on a peer-to-peer control that avoids intermediaries, and guarantees freedom of exchanges. It has been argued that these ‘emergent technologies’ may ‘empower several actors,’ including small States, and categories that were previously excluded from the traditional financial system, such as migrants, and temporary guest workers who can use this system for remittances.²⁸ In other words, these technologies create a new ‘governance’, which is in principle open to everyone, including people who previously had a weak access to the financial system, but also to criminals.

We know that not *all that glitters is gold*. We also know not everything online is the truth, is real, is fact. Why should we assume Bitcoin is genuine when it exists in a world full of fraud and disinformation by design?

The potentially erratic valuation of virtual currencies is, for example, an element of risk. As explained in the 2016 IMF report on virtual currencies, they ‘are not likely to be adequate stores of value given the volatility in their exchange rates to fiat money.’²⁹ Websites of exchange providers might be also at risk of being hacked.³⁰ For our purposes, however, another kind of vulnerability is of interest: the fact that Bitcoins can be exploited by criminal organisations to launder money, support terrorist organisations, fuel drug trafficking. The Financial Action Task Force on anti-money laundering issued a pivotal report on virtual currencies just a year after the preceding one of 2014 containing a first assessment of the phenomenon, which we have already mentioned. The international body, which is not an international organisation but belongs to the new financial architecture established at the international level,³¹ explained risks

²⁶ blogs.imf.org/2018/03/13/addressing-the-dark-side-of-the-crypto-world/

²⁷ www.imf.org/en/News/Articles/2017/09/28/sp092917-central-banking-and-fintech-a-brave-new-world

²⁸ M. Campbell-Verduyn, *What are blockchains and how are they relevant to governance in the global political economy?*, in M. Campbell-Verduyn, *op. cit.*, 6 ff.

²⁹ IMF, *Fintech and Financial Services: Initial Considerations*, www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2017/06/16/Fintech-and-Financial-Services-Initial-Considerations-44985, 26.

³⁰ See, for example, the case of Mt. Gox, the world exchange provider based in Tokyo, suddenly in 2014 filed for bankruptcy in Japan as it had lost 850,000 BTC in a suspected hack. Thousands of Bitcoins suddenly disappeared, and evidence seem to show that it was an employee the author of the fraud. K. Jia, F. Zhang, *Between liberalization and prohibition. Prudent enthusiasm and the governance of Bitcoin/blockchain technology*, in Campbell-Verduyn, *op. cit.*, 95.

³¹ See S. De Vido, *The Financial Stability Board and New Forms of Governance*, in M. Waibel (ed.), forthcoming for the Hague Academy of International Law.

and vulnerabilities of VC to money laundering and terrorist financing, and how to apply the risk-based approach elaborated in the field of anti-money laundering and countering terrorist financing to the virtual currencies context.³² Transactions using Bitcoins can be used to ‘cash out’ cybercrime proceeds, even though the data available cannot either confirm or disprove this argument.³³

The reasons why VC can be exploited by criminals can be summarised in three words: anonymity, internet, and fragmentation. The Bitcoins protocol does not require or provide identification and verification of the participants, and no authority checks the identity of those mining and trading. Internet is now commonly used to make cross-border payments and funds transfers, but VC rely on complex infrastructures of several entities in more than one jurisdiction. In international law, the issue is of utmost interest. Jurisdiction is primarily territorial, but it is difficult to propose a straightforward answer when using internet, which relativises the concept of ‘territory.’³⁴ Furthermore, the historical transaction records that are generated on the blockchain by the underlying protocols ‘are not necessarily associated with real world identity.’³⁵

The Silk road case in the US is illustrative of the vulnerabilities of these currencies to money laundering and terrorism financing.³⁶ Silk Road was a famous illegal goods-trading website, situated in the Dark Web, a part of the Deep Web that refers to content that is not indexed by search engines like Google, which allowed people to buy illicit products, such as drugs and weapons, without revealing the identity of the persons involved in the transaction.³⁷ The most favourite means of payment was using Bitcoins. Founded in February 2011 by a young man, Ross Ulbricht, the original Silk Road website made him a multi-millionaire in few years. The problem is usually how to apprehend those responsible of the illegal activities using Bitcoins. As a matter of fact, US authorities were aware of the existence of the site, but they needed time to find the person behind it. In 2015, the authorities arrested Ross Ulbricht in a public library in San Francisco, after finding the connection between his alias and his real identity. At the time of the arrest, and this is essential for what we are saying further in this contribution, he was logged into Silk Road as administrator, and his laptop had millions of dollars in Bitcoins. The domain was then seized. US authorities were competent precisely because of the traditional ground of jurisdiction: they arrested Ulbricht on US soil, doing illicit activities under US law. He was indicted with several crimes, including money laundering, drug

³² FATF, *Guidance for a Risk-Based Approach - Virtual Currencies*, June 2015.

³³ Three authors tried to assess the possibility that the system is used for launder the proceeds of a crime. See in that respect, R. Van Wegberg, J.J. Oerlemans, O. Van Deventer, *Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin*, in *Journal of financial crime*, 25, 2018, 419. Lack of data does not come as a surprise. The magnitude of money laundering is still uncertain.

³⁴ Ivi, 11.

³⁵ Ibid.

³⁶ See the entire story here blockonomi.com/history-of-silk-road/ Update November 2017. and here www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (15).

³⁷ MC Van Hout, T. Bingham, *'Silk Road', the virtual drug marketplace: a single case study of user experiences*, in *Int J Drug Policy*, 24, 2013, 385 ff., explaining the ‘displacement’ from ‘traditional’ online and street sources of drug supply. See also K. Jia, F. Zhang, *op. cit.*, 96.

trafficking, and computer hacking. Two FBI agents were also charged with money laundering and sentenced.³⁸ Ross Ulbricht was sentenced to life imprisonment.

After dealing with a case of money laundering, one might ask whether terrorists can use this means of payment. As two authors argued, it is difficult to find concrete evidence of the use of Bitcoins by terrorist groups and their supporters, but there is evidence that cryptocurrencies were connected to terrorist attacks in Europe and Indonesia.³⁹ Almost anonymous transfers of money are appealing for terrorists, which over time have proved to be able to exploit the most recent technologies to finance their activity.⁴⁰ Interestingly enough, a website such as Coindesk explains that, since most exchanges are required by law to know their customers, ‘the network is transparent, the progress of a particular transaction is visible to all,’ and ‘this makes bitcoin not an ideal currency for criminals, terrorists or money-launderers.’⁴¹ In July 2017, however, an international operation led by the United States seized AlphaBay, an online criminal market on the web. It sold firearms, toxic chemicals, illegal drugs, and exchanged more than 1 billion dollars in crypto-currencies before being closed.⁴²

2.4. *To Regulate or not to Regulate?*

Since the very beginning, the key question was whether or not VC should be regulated, and if so, how. Considering the nature of VC, it is clear that they cannot be directly regulated, absent a centralised authority.⁴³ Countries have acted in different ways in response to these new means of payments. On the one hand of the spectrum, regulation has meant a total ban to the use of these currencies. Hence, for example, Ecuador, Bolivia and Russia banned Bitcoins.⁴⁴ Despite what can be found in some websites,⁴⁵ two authors argued that China, which counted for the 50 per cent of the computation power by 2016, has not been totally restrictive with regard to Bitcoins: whereas the government warned against the risks of Bitcoins, the Peoples’ Bank of China declared to be ready to issue digital currencies.⁴⁶ On the other hand of the spectrum, there is non-regulation, which better corresponds to the initial intentions of those who created these currencies, but cannot prevent these currencies to become means of exchange to be exploited by money launderers and terrorism financiers. Between total ban and (almost) total freedom, countries have adopted different approaches. To regulate VC might mean to subject the connected activities to tax law, which goes beyond the scope of this

³⁸ They stole Bitcoins during the Bitcoins probe. www.reuters.com/article/us-usa-cyber-silkroad/ex-agent-in-silk-road-probe-gets-more-prison-time-for-bitcoin-theft-idUSKBN1D804H

³⁹ A.S.M. Irwin, G. Milad, *The Use of Crypto-Currencies in Funding Violent Jihad*, in *Journal of Money Laundering Control*, 19, 2016, 407 ff.

⁴⁰ See S. De Vido, *Strumenti giuridici di controllo nel contrasto del finanziamento al terrorismo internazionale*, Padova, 2012.

⁴¹ www.coindesk.com/information/what-is-bitcoin/

⁴² C. Lagarde, blogs.imf.org/2018/03/13/addressing-the-dark-side-of-the-crypto-world/

⁴³ *Virtual or virtueless? The evolution of money in the digital age*, Lecture by Yves Mersch, Member of the Executive Board of the ECB, Official Monetary and Financial Institutions Forum, London, 8 February 2018, www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180208.en.html

⁴⁴ K. Jia, F. Zhang, *op. cit.*, 98.

⁴⁵ www.bloomberg.com/news/articles/2018-03-19/is-this-legal-making-sense-of-the-world-s-cryptocurrency-rules.

⁴⁶ K. Jia, F. Zhang, *op. cit.*, 99.

analysis and will not be dealt with further,⁴⁷ or to subject exchange providers to anti-money laundering requirements. It is the case of the United States, where there is a low level of regulation, mainly for the purposes of AML. Hence, the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) considers businesses transacting bitcoins as money services businesses, subject, among others, to AML regulation.⁴⁸ The State of New York developed a sort of 'license' for Bitcoins, which has been object of a precise regulation.⁴⁹ Another country that saw the development of Bitcoins, Japan, amended in 2017 the Payment Services Act of 2009 in order to include 'virtual currency exchange services' within its scope of application. In particular, these services, which include the purchase and sale of a virtual currency or exchange with another virtual currency; intermediary, brokerage or agency service; management of users' money or virtual currency, must be registered.⁵⁰ The translation provided into English of the original Japanese seems to support the argument that VC are now considered as legal tender in Japan; nonetheless, as confirmed by some scholars, payments using Bitcoins are not always allowed, hence it cannot be considered, strictly speaking, as a legal tender such as Yen. In Sweden, VC exchange providers have had an obligation to register since 2012.⁵¹ In Australia, the Anti-Money Laundering and Counter-Terrorism Financing amendment act 2017, known as 'Bitcoin bill', was approved by both Houses and got Royal Assent, and subjected digital currency exchange providers to anti-money laundering requirements.⁵²

The actions undertaken by States respond to the recommendations of the FATF, which, in its 2014 report, argued that FATF Recommendations should be applied to 'convertible VC exchanges and any other type of entities that act as nodes where convertible VC activities intersect with the regulated fiat currency financial system.'⁵³ As we argued elsewhere,⁵⁴ Bitcoins should be regulated as much as all the movements of money are regulated in the world for the purposes of anti-money laundering and counter-terrorism financing. We were, and still are convinced, that it is not conceivable to have anonymous accounts, although virtual,

⁴⁷ The European Court of Justice, in a judgment of 22 October 2015 (C-264/14), argued that transactions involving non-traditional currencies, which are not legal tender in one or more countries, in so far as those currencies have been accepted by the parties to a transaction as means of payment, are financial transactions and therefore exempt from the VAT system.

⁴⁸ D. Rodima-Taylor, W.W. Grimes, *Cryptocurrencies and digital payment rails in networked global governance. Perspectives on inclusion and innovation*, in M. Campbell-Verduyn, *op. cit.*, 120-121.

⁴⁹ www.dfs.ny.gov/

⁵⁰ Virtual currency is defined as: 'Property value (limited to that which is recorded on an electronic device or any other object by electronic means, and excluding the Japanese currency, foreign currencies, and Currency-Denominated Assets; the same applies in the following item) which can be used in relation to unspecified persons for the purpose of paying consideration for the purchase or leasing of goods or the receipt of provision of services and can also be purchased from and sold to unspecified persons acting as counterparties, and which can be transferred by means of an electronic data processing system.' [www.japaneselawtranslation.go.jp/law/detail/?ft=2&re=2&dn=1&yo=&ia=03&al\[\]=P&alpha_x=8&alpha_y=19&ky=&page=10](http://www.japaneselawtranslation.go.jp/law/detail/?ft=2&re=2&dn=1&yo=&ia=03&al[]=P&alpha_x=8&alpha_y=19&ky=&page=10)

⁵¹ archive.riksbank.se/Documents/Rapporter/Riksbanksstudie/2013/rap_riksbanksstudie_The_Swedish_retailpayment_market_130605_eng.pdf and www.bitcoin.se/2012/12/04/finansinspektionen-klassar-bitcoin-som-betalningsmedel/

⁵² www.austrac.gov.au/news/digital-currency-exchange-providers-register-online-austrac

⁵³ FATF, *Guidance for a Risk-Based Approach*, 12.

⁵⁴ S. De Vido, *Network Regulation of Cross-Border Economic Crime*, in *Kobe University Law Review*, 48, 2014, 97.

in the global financial market of today. This situation would allow unidentified and unregulated subjects to have a competitive advantage compared to traditional financial institutions. This is the approach adopted by the new EU AML Directive, which is the focus of the second part of this work.

3. The new V AML Directive and virtual currencies

The new V AML Directive is the outcome of a long process of negotiation to amend, and *not to* repeal, the IV AML directive. The IV AML Directive was negotiated and then adopted to transform the FATF recommendations of 2012, non-binding, into secondary EU law, which is binding for EU member States. The Directive was adopted in 2015, after three years FATF revised its recommendations. Basically, from the very moment of its adoption, the Directive needed to be amended as a reaction to the development of VC and to the numerous terrorist attacks on EU soil.⁵⁵ The reform of the IV AML Directive must be analysed in the context of the ongoing debate on virtual currencies, which has involved several EU institutions, along with national central banks.

3.1. The EU and virtual currencies: an ongoing debate

Several EU institutions have presented reports and opinions on VC. In a report of 2015, the European Central Bank (ECB) clarified that, despite the use of the word ‘currency’, VC do not belong ‘to the world of money or currency as used in economic literature, nor is virtual money currency money, currency or currency from a legal perspective.’⁵⁶ The ECB has adopted a quite restrictive approach on VC, and in its website it has highlighted risks and vulnerabilities for consumers, and defined these currencies as ‘speculative assets.’⁵⁷

In February 2018, the European Supervisory Authorities (ESAs) for securities (ESMA), banking (EBA), and insurance and pensions (EIOPA) issued a joint warning to consumers regarding the risks of buying VC. The statement dealt with the risks of buying and trading VC, emphasising the extreme volatility and bubble risks associated to these currencies.⁵⁸ Warnings against the use of VC have come from central banks and supervisory authorities in the EU, as well, such as the German Federal Financial Supervisory Authority, the Banque de France, the Dutch and Belgian central bank and supervisor.⁵⁹ The Italian central bank, both in 2015⁶⁰ and 2018,⁶¹ recommended customers and financial institutions to consider the risks of VC while dealing with them.

While financial bodies have mainly focused on the financial vulnerability of the currencies, especially their volatility, the European Parliament has stressed

⁵⁵ See the analysis in that respect by A. Minto, A. Urbani, *Recent trends in designing the EU anti-money laundering regulatory landscape: the Fourth AML Directive between lights, shadows and future perspectives*, in *Law and Economics Yearly Review*, 5, 2016, 151 ff.

⁵⁶ ECB, *Virtual currency schemes – a further analysis*, Frankfurt, 2015, 23.

⁵⁷ www.ecb.europa.eu/explainers/tell-me/html/what-is-bitcoin.en.html

⁵⁸ ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies, February 2018.

⁵⁹ ECB, *Virtual currency schemes*, *cit.*, 30.

⁶⁰ www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/AVVERTENZA_VALUTE_VIRTUALI.pdf

⁶¹ www.binck.it/docs/librariesprovider8/default-document-library/avvertenze-valute-virtuali-2018.pdf

the risks of money laundering and terrorism financing. In 2016, the European Parliament adopted a resolution in which it focused on the weaknesses of the VC system, including ‘the absence of a flexible, but resilient and reliable, governance structures or indeed a definition of such structures,’ the high volatility of VC and potential for speculative bubbles, and, in particular, ‘the potential for ‘black market’ transactions, money laundering, terrorist financing, tax fraud and evasion and other criminal activities based on the ‘pseudonymity’ and ‘mixing services’ that some such services offer and the decentralised nature of some VC, bearing in mind that the traceability of cash transactions tends to be much lower still.’⁶² A recent report, commissioned by the European Parliament’s Policy Department for Citizens’ Rights and Constitutional Affairs, explored the terrorism financing risks of virtual currencies, including cryptocurrencies such as Bitcoins.⁶³ As we anticipated, it is difficult to measure the extent of the exploitation by terrorists of these means. Nonetheless, the case of Kosovo national *Ardit Ferizi* which tried to install malware to obtain information of US government workers later published by the Islamic State, is an example of how cybercrime, terrorism and use of VC can interact.⁶⁴

3.2. The European Commission’s proposal for the V AML Directive

Given the inputs coming from the ECB, and the European Parliament, the European Commission started the process to amend the IV AML Directive more than one year before the deadline for the transposition of the same Directive into the national legal systems. In its 2016 Communication, the European Commission acknowledged, on the one hand, the important steps forward undertaken through the reform of the EU anti-money laundering system, and, on the other hand, it stressed how the terrorist threat had ‘grown and evolved recently:’⁶⁵

[...] by advances in technology and communications, the globally interconnected financial system makes it simple to hide and move funds around the world, by quickly and easily setting up layer upon layer of paper companies, crossing borders and jurisdictions and making it increasingly difficult to track down the money. Money launderers, tax evaders, terrorists, fraudsters and other criminals are all able to cover their tracks in this way.

At the time of the Communication, transposition into national legal systems of the Directive was ongoing – deadline was indeed on 26 June 2017 – hence the Commission encouraged States to accelerate the process in order to achieve full transposition by 1 January 2017, and to take into consideration the proposed amendments which could have been included in the process of transposition itself. The Commission proposed amendments to the IV AML Directive, and to Directive 2009/101/EC on company rules as well.⁶⁶

⁶² European Parliament resolution of 26 May 2016 on virtual currencies (2016/2007(INI), 26 May 2016, para. 2.

⁶³ European Parliament, Virtual currencies and terrorist financing: assessing the risks and evaluating responses, May 2018.

⁶⁴ Ivi, 43.

⁶⁵ Proposal for a Directive of the European Parliament and of the Council 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 Directive 2009/101/EC, 5 July 2016, (2016) 450 final, para. 1.

⁶⁶ Directive 2009/101/EC of the European Parliament and of the Council of 16 September 2009 on coordination of safeguards which, for the protection of the interests of members and

Legal bases of the proposed Directive were found in Articles 114 (approximation of laws) and 50 TFEU (freedom of establishment). Since they are the same legal bases used for the amended acts, they will not be discussed further in these pages.

For the purposes of this contribution, two elements of the proposal are relevant here. The first one is the inclusion of virtual currency exchange platforms, and of custodian wallet providers, as obliged entities for the purposes of anti-money laundering. The second interesting aspect is the proposal to enable financial intelligence units to request information that might be relevant for AML and CTF from all the obliged entities, with the purpose to reinforce cooperation among these entities within Europe. FIUs usually receive information on the basis of a report of suspicious transactions. The amendment aimed at allowing FIUs to ask additional information from obliged entities, and 'have access on a timely basis to the financial, administrative and law enforcement information they require to undertake their functions properly even without there having been a suspicious transaction report.'⁶⁷

3.3. *The adoption of the Directive*

Discussions within the Council lasted almost two years. In 2016, the European Central Bank, who had previously issued a statement concerning virtual currencies, supported the European Union action and recommended further improvements to some provisions of the proposal that were then incorporated in the final draft.⁶⁸ In particular, the ECB emphasised that virtually currencies cannot be considered as legally established currencies or money, and that they should be considered as means of exchange rather than as mere means of payment as initially conceived by the European Commission.

On 7 November 2016, the European Parliament co-rapporteurs presented their draft report on the Commission proposal.⁶⁹ The Council adopted compromise positions, and finally gave its negotiating mandate on 13 December 2016. A compromise text proposed by the Presidency was then presented to the delegations.⁷⁰ The Council rejected the article on the amendments to Directive 2009/101/EU concerning beneficial ownership, and added amendments to

third parties, are required by Member States of companies within the meaning of the second paragraph of Article 48 of the Treaty, with a view to making such safeguards equivalent, *GU L 258/11*, 1.10.2009.

⁶⁷ (2016) 450 final, para. 5 c).

⁶⁸ Opinion of the European Central Bank of 12 October 2016 on a proposal for a directive of the European Parliament and of the Council 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 Directive 2009/101/EC (CON/2016/49) (2016/C 459/05).

⁶⁹ See the procedure in [www.europarl.europa.eu/RegData/etudes/BRIE/2017/607260/EPRS_BRI\(2017\)607260_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/607260/EPRS_BRI(2017)607260_EN.pdf)

⁷⁰ General Secretariat of the Council To: Delegations No. Cion doc.: COM(2016) 450 final Subject: Proposal for a Directive of the European Parliament and the Council 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 Directive 2009/101/EC, Negotiating mandate.

Directive Solvency II 2009/138/EC,⁷¹ and on the Fourth Capital Requirement Directive 2013/36/EU.⁷²

On 28 February 2017, the Committee on economic and monetary affairs and Committee on Civil Liberties, Justice and Home Affairs adopted their report together with a mandate for negotiations with the Council in trilogue, which was announced in plenary in March 2017. The European Parliament proposed several amendments to the Commission's proposal, which however did not significantly impact on the provisions related to VC. Several trilogue meetings were necessary before the institutions were able to come to an agreement which was achieved on 20 December 2017. The rejection of the amendments to the Directive 2009/101/EU was confirmed.

Among the amendments to the IV AML Directive that will significantly contribute to the protection of the financial system from risks of money laundering and terrorism financing, and which will not be object of analysis here, it is worth mentioning the beneficial ownership registers for legal entities within each Member State, which will be made public, and which will be directly interconnected to facilitate cooperation. Furthermore, the European Commission will keep the update of a list of third countries, which are considered as high risk because they have low transparency on beneficial ownership information, no appropriate sanctions or do not either cooperate or exchange information. The cooperation between financial intelligence units is also reinforced thanks to the new provisions.

3.4. Provisions on virtual currencies in the V AML Directive

The V AML Directive includes, among the obliged entities for the purposes of AML and CTF, virtual currency exchange platforms (VCEPS) and custodian wallet providers (CWPs). It means that these entities must apply customer due diligence requirements and adopt all the measures that have been conceived to prevent the misuse of the financial system for purposes of criminal activity. As acknowledged in the preamble:

Providers engaged in exchange services between virtual currencies and fiat currencies (that is to say coins and banknotes that are designated as legal tender and electronic money, of a country, accepted as a medium of exchange in the issuing country) as well as custodian wallet providers are under no Union obligation to identify suspicious activity. Therefore, terrorist groups may be able to transfer money into the Union financial system or within virtual currency networks by concealing transfers or by benefiting from a certain degree of anonymity on those platforms. It is therefore essential to extend the scope of Directive (EU) 2015/849 so as to include providers engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet providers.⁷³

⁷¹ Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), *GUL* 335, 17.12.2009.

⁷² Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC Text with EEA relevance, *GUL* 176, 27.06.2013.

⁷³ Preamble, recital no. 8.

In response to the opinion of the ECB, the directive clarifies that virtual currencies cannot be confused with electronic money, and that, even though they are used as means of payment, they can also be used for other purposes, such as means of exchange, investment, store-of-value product, or use in online casinos.⁷⁴ This recital of the preamble is mirrored in the definition provided in article 1, d, letter 18, of the V AML Directive:

‘[V]irtual 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 or legal persons as a means of exchange and which can be transferred, stored and traded electronically.

It seems that what matters is the *de facto* acceptance of the currency as means of payment. VC might not have the legal status of a currency, but *de facto* it is considered as such by those who use it as a means of payment and / or exchange. The Directive also defines ‘custodian wallet providers,’ an expression which identifies those entities providing ‘services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies.’⁷⁵

As a consequence of these provisions, exchange platforms and CWP’s must, among the numerous obligations that mirror the FATF recommendations, assess the identity of the customers, avoid anonymous accounts, and keep records of the information. One can object that, even though an account is anonymous, upon request of the authorities, the providers must communicate the IP that is necessary to identify the owner of a specific wallet. Nonetheless, even if it is the case, and the provider is willing to cooperate – which is not thus straightforward – it is also true that this is a *post facto* measure, not a preventive measure, which is on the contrary the purpose of the measures that have been adopted over the years to prevent money laundering and terrorism financing.

Furthermore, Article 47 (1) of the IV AML Directive is replaced, according to the V AML Directive, by the following:

Member States shall ensure that providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers, are registered.⁷⁶

As I explained before, it was precisely what some countries have decided to do with regard to VC.

Provisions on cooperation among FIUs and access to information might also be relevant for the purposes of controlling the activity of exchange platforms and custodian wallet providers. Furthermore, the Directive requires the elaboration of a report, scheduled by 11 January 2022, and every three years thereafter, containing, *inter alia*, the specific measures adopted and the mechanisms set up at EU and Member States’ level to prevent and address emerging problems and new developments presenting a threat to the Union Financial system, follow-up actions undertaken at EU and Member States’ level, and an evaluation of how fundamental rights have been respected.⁷⁷ This provision amends Article 65 of the IV AML

⁷⁴ Preamble, recital no. 10.

⁷⁵ Article 1, d, number 19.

⁷⁶ Article 1, para. 29

⁷⁷ Article 1, para. 41.

Directive. At the same time, the legal instrument allows a further development. The report shall be accompanied ‘if necessary,’ and the language is extremely vague here, by ‘appropriate legislative proposals, including, where appropriate, with respect to virtual currencies, empowerments to set-up and maintain a central database registering users’ identities and wallet addresses accessible to FIUs, as well as self-declaration forms for the use of virtual currency users, and to improve cooperation between Asset Recovery Offices of the Member States.’ This seems to mirror the decision of the State of New York, which opted for a registration of the businesses dealing with Bitcoins. On the one hand, these measures seem to contradict the spirit of VC, born to precisely escape the traditional financial system;⁷⁸ on the other hand, however, it seems to correspond to a process of ‘normalisation’ that we mentioned at the beginning, with even businesses trading in Bitcoins accepting forms of voluntary AML compliance.⁷⁹

Deadline for the transposition of the EU Directive into the national legal systems of EU Member States is 10 January 2020, although some countries have already complied with the new provisions, anticipating the outcome of the Directive, following the recommendations of the FATF. In Italy, for example, the Italian Parliament adopted in 2017 a legislative decree, No. 90 of 25 May 2017,⁸⁰ through which Italy transposed the previous IV AML Directive, adding, among the obliged entities, ‘service providers related to the use of virtual currencies,’ which can include both the exchangers and the CWP, although regulation is limited to their activity of ‘converting VC from or into fiat currencies.’⁸¹

4. Legal challenges deriving from the regulation of VC at EU level

VC service providers are now formally bound by AML requirements at European Union level. The EU Directive needs to be transposed into the national legal systems in order AML requirements to be effective, however the path has been clearly lit, as anticipated by the European Banking Authority and by the European Parliament. Let us turn to the legal challenges deriving from the regulation of VC at EU level. The obliged entities are both those who convert VC into fiat currencies and *viceversa*, and custodian wallet providers. It means that these entities must, among other obligations, know their clients, and keep records of the data associated with the operations they undertake. Obligated entities must also avoid anonymous accounts. What about pseudonyms? Provided that the data on the clients are stored by the providers, AML requirements are respected without

⁷⁸ This might encourage some of these activities to go underground.

⁷⁹ M. Campbell-Verduyn, M. Goguen, *The mutual constitution of technology and global governance. Bitcoin, blockchains, and the international anti-money-laundering regime*, in M. Campbell-Verduyn, *op. cit.*, 82.

⁸⁰ Decreto Legislativo 25 maggio 2017, n. 90, Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006, in G.U. no. 140, 19.06.2017, Suppl. Ord. No. 28, Article 1(5) letter i).

⁸¹ On the ‘minimalist’ although pragmatic approach of the Italian law, see A. Urbani, *La disciplina antiriciclaggio alla prova del processo di digitalizzazione dei pagamenti*, in *Rivista di diritto bancario*, 5, 2018, p. 13. See also P. Valente, *Bitcoin and virtual currencies are real: are regulators still virtual?*, in *Intertax*, 541 ff.

interfering with the character of partial anonymity of VC. Regulation is not devoid of criticism though.

The first legal challenge is related to jurisdiction. Where should the VC providers and custodian wallet providers be located in order to fall under the scope of the Directive? The answer is obvious in its simplicity: on EU soil; but it is complex when it comes to contextualise these currencies in the virtual world, which almost by definition does not have frontiers. The Directive does not contain indeed a provision similar to the one included in the General Data Protection Regulation of 2016, which would have been expanded the territorial reach of the V AML Directive.⁸² Article 3 of the aforementioned regulation reads as follows:

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not [...]
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

There is no similar provision in the V AML Directive. A provision that would have mirrored the one included in the regulation would have been a huge step forward, and would have been an important attempt to respond to the challenges posed by the virtual world.

74

The second legal challenge is related to the former, and concerns the place where operations are conducted. It was also pointed out by the European Central Bank in its opinion to the European Commission's proposal for the V AML Directive:

In this context, the ECB also mentions that digital currencies do not necessarily have to be exchanged into legally established currencies. They could also be used to purchase goods and services, without requiring an exchange into a legally established currency or the use of a custodial wallet provider. Such transactions would not be covered by any of the control measures provided for in the proposal and could provide a means of financing illegal activities.⁸³

In other words, the regulation of VC concerns the moment of transition from one world to the other: the virtual to the real one, and *viceversa*. If the exchange happened before the entry into force of the national legislation implementing the Directive, the transactions conducted using Bitcoins will be completely outside the scope of the Directive. Could the States broaden the scope of the Directive in their activity of transposition into the national legal systems? Possibly yes, although always in respect of international law. The example of the regulation on privacy at European level could guide the formulation of provisions at national level.⁸⁴

⁸² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

⁸³ Opinion ECB, para. 1.1.1.

⁸⁴ There is also a legal debate on the fact that blockchains might fall under the scope of the General Data Protection Regulation, since they store personal data. Regulation on privacy might restrict access to bitcoins websites. www.express.co.uk/finance/city/965116/Bitcoin-GDPR-price-ripple-cryptocurrency-ethereum-BTC-to-USD-XRP-news

The third legal challenge pertains to a specific instrument, the so-called initial token or coin offerings (ICO). Thanks to a ICO, ‘a venture offers a stock of specialized crypto tokens for sale with the promise that those tokens will operate as the medium of exchange when accessing the venture’s products,’ hence the sale of tokens constitutes the initial capital to fund the development of a business.⁸⁵ In the Bitcoins magazine, ICO is defined as ‘a fundraising mechanism in which new projects sell their underlying crypto tokens in exchange for bitcoin,’ and it is compared to ‘an Initial Public Offering (IPO) in which investors purchase shares of a company.’⁸⁶ ICOs are not covered by the V AML Directive, even though they might constitute fertile ground for setting up criminal business activities.⁸⁷

5. Concluding Remarks

The response of the EU to the risks of ML and TF posed by VC, in particular Bitcoins, was in favour of regulation. The adoption of the V AML Directive did not come as a surprise, given the declarations and the opinions of EU institutions and national central banks in the previous years. Regulation is surely fundamental, and can prevent VC from being exploited for criminal purposes. ‘Traditional’ financial institutions have not always been regulated for the purposes of AML, but they have started to be as soon as the connection existing between the use of the financial system and financial crimes became clear. It seems thus an obvious consequence that also VC exchange platforms and custodian wallet providers, whose characteristics of anonymity and volatility have proved to be enticing to criminals, needed regulation. Nonetheless, despite the interesting achievement, the new Directive has its own limits, because it only refers to AML requirements applicable in the moment in which the virtual world meets the real one, namely when fiat currencies are transformed into VC and viceversa. The Directive neither addresses operations using Bitcoins, nor new mechanisms such as ICOs.

VC, and the technology that backs them, are surely a new emergent technology which must not be in principle demonised. The ongoing process that we can see in many countries, and in the EU as well, is a form of ‘normalisation’ of VC, even though the main purpose of the creation of VC was the necessity to escape from the laces imposed by the traditional financial system, and to develop a system based on trust among peers. In the fight against money laundering, which can be conceived as a public interest in the Europe – Europe broadly speaking, including the Council of Europe’s member States – regulation seems not only fundamental but also unavoidable. The fact that, as reaction to the increasing regulation, VC go ‘darker,’ trying to escape any attempt of regulation, does not justify a loose system of control, which would be an inexplicable exception compared to the regulation to which financial institutions are normally subjected. The consequences of this process of ‘regulation’ of VC are still to be assessed.

⁸⁵ C. Catalini, J.S. Gans, *Initial Coin Offerings and the Value of Crypto Tokens*, NBER Working Paper No. 24418, March 2018.

⁸⁶ bitcoinmagazine.com/guides/what-ico/

⁸⁷ In the US, the Securities and Exchange Commission issued an investigative report in July 2017 ‘cautioning market participants that offers and sales of digital assets by “virtual” organizations are subject to the requirements of the federal securities laws.’ Such offers and sales, promoted by businesses that use distributed ledger or blockchain technology, have been referred to, among other things, as “Initial Coin Offerings” or “Token Sales.” See press release, 25 July 2017, www.sec.gov/news/press-release/2017-131

Whether this regulation will completely jeopardise the very existence of VC, leading to their disappearance, or whether normalisation will emphasise the potential of the technology behind VC, only time will tell.