Georgios Pavlidis

International Regulation of Virtual Assets under FATF's New Standards

NUP Jean Monnet Working Paper Series

2/2021

With the support of the Erasmus+ Programme of the European Union

Neapolis University Pafos

The NUP Jean Monnet Working Paper Series can be found at:

https://www.nup.ac.cy/jean-monnet-chair/working-papers/

Publications in the Series should be cited as:

AUTHOR, TITLE, NUP JEAN MONNET WORKING PAPER NO. x/YEAR [URL]

Copy Editor: G. Pavlidis

Neapolis University Pafos, School of Law

Pafos, 8042, Cyprus

International Regulation of Virtual Assets under FATF's New Standards

Abstract

This paper aims to critically examine two significant developments for the regulation and supervision of virtual assets and virtual assets services providers: the amendment of the Financial Action Task Force (FATF) Recommendation No 15 in October 2018 and the adoption of an Interpretative Note in June 2019. We argue that new FATF standards constitute an appropriate response to money laundering and terrorist financing risks associated with virtual assets, but that they must be followed by firm, consistent and effective implementation at the national level, in order to reduce the risk of jurisdiction-shopping by money launderers and terrorism financiers.

Keywords

Virtual assets, Crypto-assets, Virtual asset service provider (VASP), Initial coin offering (ICO), Money laundering, Financial Action Task Force (FATF)

1. The Rise of Virtual Assets and the Associated Money Laundering Risks

The Financial Action Task Force (FATF), the principal international forum and standard-setting inter-governmental body in the areas of anti-money laundering and countering the financing of terrorism (AML/CFT), has defined virtual assets as 'digital representations of value that can be digitally traded or transferred and can be used for payment or investment purposes, including digital representations of value that function as a medium of exchange, a unit of account, and/or a store of value'(FATF, 2018a; FATF, 2018b).

The FATF definition covers a wide range of assets, the existence and value of which rely on the use of cryptography and distributed ledger technology (BIS, 2018; Nair, 2019; Dallyn, 2017; Swartz, 2018; Corradi and Höfner, 2018). These assets fall into three main categories: (a) payment/exchange-type tokens, including the so-called virtual currencies, such as Bitcoin and Litecoin; (b) investment/security-type tokens, such as Bankera; and (c) utility-tokens used to access applications or services (EBA, 2019).

Depending upon the form of crypto-asset, there may be different types of virtual asset service providers (VASPs) available, such as providers of financial services for initial coin offerings (ICOs), wallet providers and virtual currency exchanges. In all these cases, virtual assets are neither issued nor guaranteed by central banks or public authorities, and they do not constitute claims on central banks. Thus, they tend to be distinguished from real currency that is designated as legal tender [1] though the idea of central bank-issued cryptocurrency has been explored by some central banks, including the Swedish Central Bank in its E-Krona project (Sveriges Riksbank, 2017; Yanagawa and Yamaoka, 2019).

Despite the risks of investing in ICOs (fraud, market manipulation, operational resilience, hacks and cyber-attacks, money laundering and terrorist financing) and the efficiency problems in the cryptocurrencies market (Vidal-Tomas and others, 2019; Rice and Williams, 2019), demand grew in 2018, with a record-breaking US$15 billion raised in the first semester of 2018, with blockchain platforms being the most successful investment products [2]. Since then, ICO proceeds have dropped, but still "at the start of 2020, over 5,100 crypto-assets exist with a total market capitalization exceeding $250 billion" (European Parliament, 2020).

To deal with the rise of virtual assets and VASPs, three main approaches have been put forward (FATF, 2014). The first approach places emphasis on the potential of virtual assets for financial innovation (Burniske and Tatar, 2017; Chiu, 2017); the second stresses the risks associated with the misuse of virtual assets and their potential to serve as a powerful tool for criminals and terrorist financiers to conceal and move illicit funds (Mikhaylov and Frank, 2018; Copeland and others, 2019; Whyte, 2019); a third group of observers view virtual assets as a passing fad

or bubble [3]. There is, however, a consensus that the scale of the risks and the relatively small size of the market for crypto-assets would not justify a policy of cracking down on digital currencies (Financial Stability Board, 2018; Stokes, 2012); instead, vigilant monitoring and assessment of the emerging risks by global regulators, such as FATF, is necessary to prevent criminals from taking advantage of the anonymity attached to private/public keys of crypto-assets (Spithoven, 2019; Edwards and others, 2019).

2. Approaches to Regulating Virtual Assets

Some jurisdictions, including global financial centers, already regulate activities in crypto-assets (Wong, 2019; Spafford, Stanaway and Chung, 2019). In the US, cryptocurrency exchangers and administrators are already considered as money transmitters for AML/CFT purposes; they are required to register with the Financial Crimes Enforcement Network (FinCEN), as well as to implement customer identification programs and file reports required under the Bank Secrecy Act [4] (Nolan and others, 2018; Hughes, 2017), and in particular suspicious transaction reports (SAR) (FinCEN, 2013). FinCEN has recently updated and consolidated its rules, guidance and rulings on virtual currencies (FinCEN 2019a; FinCEN 2019b), while a joint statement by FinCEN, the U.S. Securities and Exchange Commission and the U.S. Commodity Futures Trading Commission provided further guidance on the definition of digital assets (FinCEN, SEC and CFTC, 2019).

With the number of SAR filings involving virtual currency on the rise (over 11,000 SARs filed by VASPs in 2019 following the issuance of the FinCEN guidance), the challenge will be to quickly 'identify emerging threats and typologies [...] for financial institutions to better understand and effectively report on these threats' (Blanco, 2018). Nevertheless, depending on the particular type of financial institutions involved, there may be slight differentiations in reporting requirements in the US [5]. It has been correctly pointed out that 'the absence of bright line tests makes ascertaining the regulatory status of particular customer types and activities labour-intensive' (Holman and Stettner, 2018). Furthermore, procedures developed by VASPs in relation to key aspects of AML compliance, in particular Know Your Customer (KYC) regulations, may vary widely, 'with some being very weak' (Massad, 2019; Office of the New York Attorney General, 2018).

At the EU level, the European Securities and Markets Authority (ESMA) and the European Banking Authority (EBA) have both recommended that VASPs and providers of financial services for ICOs fall within the scope of AML/CFT obligations (ESMA, 2019; EBA, 2019; European Commission, 2018). The Fifth Money Laundering Directive already requires crypto-asset exchanges and custodian wallet providers to exercise due diligence and apply KYC requirements, thus increasing the traceability of crypto-asset transactions in the EU (Miseviciute,

2018)[6]. As far as the registration and licensing of VASPs is concerned, regulators in all EU member states require authorization for the establishment of a virtual currency exchange, but the strictness of national regulations may vary (Demertzis and Wolf, 2018). Some countries, such as the UK (former member since 31 January 2020) envisage regulatory approaches that go 'significantly beyond the requirements set out in the EU Fifth Anti-Money Laundering Directive', while other countries may be less on the alert (Cryptoassets Taskforce, 2018; Maxson and others, 2019).

The lack of a uniform, or at least harmonized, regulatory and supervisory approach at EU and international levels to virtual assets increases the risk of money laundering and terrorism financing (Albrecht and others, 2019; Teichmann, 2018). We argue that a global approach needs to be forged to effectively mitigate money laundering risks; 'since crypto-assets know no borders, the framework to regulate them must be global as well', as International Monetary Fund (IMF) Managing Director C. Lagarde has correctly pointed out (Lagarde, 2019). We further argue that FATF must become the forum of choice for the development of such a global framework in the AML/CFT area, given its expertise in the field and the importance of FATF's initiatives in progress (Pavlidis, 2020).

3. The FATF Forges a New International Approach

In October 2018, the FATF revised Recommendation No 15, amending its scope to cover activities involving virtual assets and calling its members to 'ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with [...] the FATF Recommendations'. This development was followed in June 2019 by the adoption of a new Interpretive Note to Recommendation No 15 (hereinafter: 'Interpretative Note'), taking into consideration constructive consultations with the private sector.

The implementation of these new standards in the context of virtual assets will be monitored by FATF, as they will become part of the framework of the mutual evaluations process, which has so far successfully encouraged the compliance of FATF member states. Despite their nature as 'soft law', FATF standards have been transposed and implemented consistently by FATF member states. In addition to being a 'transnational public policy network' (Reinicke, 1998), FATF has gained a reputation as a 'coercive institution' (Nance, 2018) through its blacklisting process (Non-Cooperative Countries and Territories – NCCT) and the mutual evaluation rounds, a very successful peer-based diagnostic monitoring process. We argue that FATF's experience and success in developing AML/CFT standards and ensuring compliance renders it an ideal forum for the development and implementation of new standards on virtual assets. Furthermore, given FATF's past record with ensuring compliance, future national initiatives and EU initiatives are expected to

be streamlined with the FATF standards on virtual assets, as part of the FATF dynamic monitoring process (Pavlidis, 2020).

3.1. The Legal Nature of Virtual Assets under the FATF Standards

The question of whether cryptocurrencies should be recognized as the subject of property rights, as well as assessing the legal status of virtual assets in general, is of great importance, since doing so determines whether and how financial services and AML/CFT rules are likely to apply (Low and Teo, 2017; Zilioli, 2020). Under the new FATF standards, virtual assets are considered to be 'property', 'proceeds', 'funds', 'funds or other assets' or a 'corresponding value' for the purposes of implementing AML/CTF measures. This removes long-standing uncertainty as to the legal nature of virtual assets and the coverage of VASPs by AML/CTF rules. It therefore constitutes a major paradigm shift, since the new definition will soon become transposed to the national regulations of FATF members, thus evolving into an international standard.

3.2. A Risk-based Approach to Virtual Assets under the FATF Standards

Since virtual assets and VASPs are now unequivocally covered by FATF standards, FATF Recommendation No 1 applies and FATF member countries have to 'identify, assess, and understand the money laundering and terrorist financing risks' that are associated with virtual asset activities. Therefore, a risk-based approach (RBA) will have to be applied to commensurate AML/CFT measures adopted with the risks identified. For example, under this approach, FATF members should apply enhanced due diligence to higher-risk convertible and decentralised virtual currencies (FATF, 2015). Under the new regime, VASPs will also have to apply an RBA, leading to effective action to mitigate those risks. Indicators of higher money laundering risk for VASPs are, among other factors: the absence of face-to-face business relationships, the possibility of pseudonymous transactions that inhibit the identification of the beneficiary, the exposure to Internet Protocol (IP) anonymizers, links to jurisdictions with weak AML/CFT controls, etc. (FATF, 2019).

3.3. Registration of VASPs under the FATF Standards

A challenge under the new FATF standards will be the licensing or registration of VASPs, defined as 'any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i. exchange between virtual assets and fiat currencies; ii. exchange between one or more forms of virtual assets; iii. transfer of virtual assets; iv. safekeeping

and/or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset' (FATF, 2018a).

Under the new Interpretative Note, registration of VASPs will have to take place 'at a minimum' in the jurisdiction where these entities are created. Consequently, VASPs may also have to be licensed or registered in the jurisdictions from which they offer products to customers or conduct operations. Thus, these jurisdictions will be able to take charge and assume a proactive role in the supervision of VASPs; nevertheless, under this model of dual or multiple supervision, effective cooperation between national supervisory bodies would be strongly required (see section 3.6).

Jurisdictions have flexibility to determine the AML/CFT category of regulated activities under which VASPs should be regulated (financial institutions, designated non-financial business or profession or another distinctive category, etc.)(FATF, 2019). In this context, the Interpretative Note correctly points out that already licensed or registered financial institutions, as defined by the FATF Recommendations, will not need a separate registration to perform VASP activities.

To comply with FATF standards, national authorities will have to identify instances of VASP activities being carried out without the necessary license or registration, in order to apply sanctions. To identify possible solicitations by unregistered entities, FATF encourages its member states to use web-scraping tools, mechanisms for public feedback, information from Financial Intelligence Units (FIUs) and reporting institutions, law enforcement and intelligence reports (FATF, 2019). Under the Interpretative Note, national authorities will also have to ensure that criminals or their associates will be prevented from 'holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a VASP'. For this reason, substantive changes in VASP ownership, operation and structure should be made conditional on the authorities' prior approval (FATF, 2019).

3.4. Regulation and Supervision of VASPs under the FATF Standards

The supervision or monitoring of VASPs for AML/CFT purposes should be adequate and effective, in order to mitigate money laundering risks associated with virtual assets. Under the FATF standards, a competent national authority, not a self-regulatory body, should supervise or monitor VASPs on a risk-based basis. This authority should have adequate powers to ensure compliance, 'including the authority to conduct inspections, compel the production of information, and impose [...] a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the VASP's license or registration, where applicable'

[7]. In line with Recommendation 35, FATF members should introduce an arsenal of criminal, civil or administrative sanctions for failing to comply with AML/CFT requirements. According to the Interpretative Note to FATF Recommendation 15, such sanctions should not only be 'effective, proportionate and dissuasive', but they should be applicable to both VASPs and their senior management.

3.5. Preventive Measures under the FATF Standards

Currently, some platforms of crypto-assets incorporate KYC functionalities, while 'others seemingly fail on having the necessary resources and processes in place to address those risks' (ESMA, 2019). Under the new standards, FATF Recommendations No 10 to No 21 would apply to VASPs under certain conditions. Firstly, the threshold above which VASPs must conduct customer due diligence for occasional transactions is fixed at USD/EUR 1,000, in accordance with Recommendation No 10. Secondly, accurate originator information and beneficiary information must be obtained and held by originating VASPs for virtual asset transfers. The information in question must be made available immediately and securely to beneficiary VASPs and, on request, to appropriate authorities. Under the new Interpretative Note to FATF Recommendation 15, the possibility of freezing action and the prohibition of transactions with designated persons and entities apply to virtual assets activities 'on the same basis as set out in Recommendation 16'.

3.6. International Cooperation Relating to Virtual Assets

Under the new standards, FATF member countries should provide the widest possible range of international cooperation for the purposes of money laundering offences, predicate offences, and terrorist financing offences, when virtual assets are involved. Information sharing between financial intelligence units and competent law enforcement authorities can help financial and criminal investigations and prevent jurisdiction-shopping by money launderers and terrorism financiers (Irwin and Turner, 2018). It is positive that the requirement of constructive and effective cooperation under FATF Recommendations No 37 to No 40 has been extended to virtual asset operations. It is also positive that, under the Interpretative Note, the exchange of information between supervisors of VASPs should be prompt and effective, 'regardless of the supervisors' nature or status and differences in the nomenclature or status of VASPs'. Monitoring and ensuring the implementation of these standards in the framework of FATF's successful mutual evaluation process will create a level regulatory playing field on the global stage.

4. Concluding Remarks

The scope of monitoring or supervision of virtual assets according to the FATF standards is limited to AML/CFT purposes and does not extend to safeguarding financial stability in general or consumer/investor protection in particular. The work of FATF is not all-encompassing and regulating virtual asset activities is a complex task involving numerous stakeholders. The new international AML/CFT regulatory environment should not impede companies from innovating, serving an increasing range of financial services and improving financial inclusion. Nevertheless, refraining from regulating virtual asset activities, especially in the AML/CFT area, is not an option. Most jurisdictions have not yet introduced specific reporting requirements for crypto-asset activities, a lack that prevents competent authorities from monitoring these activities and the AML/CFT risks arising thereof (EBA, 2019).

Such lack of a global approach increases the risk of jurisdiction-shopping by money launderers and terrorism financiers, who favour jurisdictions with weak regulation of crypto-asset activities. There is also the risk that money launderers resort to 'crypto to crypto' services, allowing for the exchange of traceable crypto-assets (Bitcoin, Ethereum) to crypto-assets that ensure anonymity in jurisdictions with weak AML/CFT controls (TRACFIN, 2019; FATF, 2019). Finally, there is the risk that money launderers resort to 'tumblers' and 'mixing services' offered on the Dark Web, which anonymize virtual assets further by combining them with non-tainted assets across multiple jurisdictions (van Wegberg and others, 2018). For all these reasons we argue that it is necessary and opportune to forge a uniform global approach to mitigate money laundering risks associated with crypto-assets in the framework of the FATF and building on FATF's initiatives in progress.

Notes

1. According to the EU definition, the term 'virtual currency' refers to 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'; see Directive 2018/843 of the European Parliament and Council of 30 May 2018 amending the Anti-Money Laundering Directive 2015/849, OJ L 156/43 of 19.6.2018.
2. Nevertheless, according to an EY study, 86% of the ICO start-ups of 2017 were below their listing price one year later, while 30% had lost all their value in that period. See EY, "Initial Coin Offerings (ICOs) The Class of 2017 – One Year Later", EY Study, 19 October 2018.
3. According to former US Federal Reserve Chairman A. Greenspan, 'you have to really stretch your imagination to infer what the intrinsic value of Bitcoin is. I haven't been able to do it. Maybe somebody else can'; Bloomberg, "Greenspan Says Bitcoin a Bubble Without Intrinsic Currency Value", Bloomberg Interview, 5 December 2013; according to 2013 Nobel Laureate economist, R. Shiller, investing in cryptocurrencies 'it's a story that I think goes way beyond the merit of the idea [...] It is more psychological than something that could be explained by the computer science department'; CNBC, "Bitcoin is a bubble and a perfect example of faddish human behavior, says Robert Shiller", 13 April 2018.
4. Bank Secrecy Act of 1970, as amended by the USA PATRIOT Act, 31 U.S.C. §§ 5311 et seq; in 2019, FinCEN assessed for the first time a civil money penalty against an individual for failure to register as a money service business; FinCEN Penalizes Peer-to-Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws, Press Release, April 18, 2019.
5. Different registration requirements are imposed to money services businesses (FinCEN), issuers, brokers and dealers of securities (Securities and Exchange Commission-SEC), brokers and dealers of commodities (Commodity Futures Trading Commission-CFTC); See 31 C.F.R. § 1010.100(ff); 15 U.S.C. §§ 78c(a); 7 U.S.C. § 1A(31).
6. See Article 1(1)(c) Directive 2018/843 of the European Parliament and Council of 30 May 2018 amending the Anti-Money Laundering Directive 2015/849, OJ L 156/43 of 19.6.2018; nevertheless, virtual-to-virtual asset exchanges do not fall within the scope of the new directive, which only covers virtual-to-fiat currency exchanges.
7. Interpretative Note to FATF Recommendation 15, paragraph 5.

References

1. Albrecht, C. and others (2019), "The Use of Cryptocurrencies in the Money Laundering Process", *Journal of Money Laundering Control*, vol. 22, pp. 210-216.
2. Bank for International Settlements (2018), "Cryptocurrencies: Looking Beyond the Hype", BIS Annual Economic Report, Basel.
3. Blanco, K. (2018), *Remarks of FinCEN Director Kenneth Blanco at the Chicago-Kent Block (Legal) Tech Conference*, FinCEN Press Release, 9 August 2018.
4. Burniske, C., Tatar, J. (2017), *Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond*, McGraw-Hill.
5. Chiu, I. (2017), "A New Era in FinTech Payment Innovations? A Perspective from the Institutions and Regulation of Payment Systems", *Law, Innovation and Technology,* vol. 9, pp. 190-234.
6. Copeland, C., Wallin, M., Holt, T. (2019), "Assessing the Practices and Products of Darkweb Firearm Vendors", *Deviant Behavior* [latest articles].
7. Corradi, F. Höfner, P. (2018), "The Disenchantment of Bitcoin: Unveiling the Myth of a Digital Currency", *International Review of Sociology*, vol. 28, pp. 193-207.
8. Cryptoassets Taskforce (2018), "Final Report", HM Treasury, Financial Conduct Authority, Bank of England, London.
9. Dallyn, S. (2017), "Cryptocurrencies as Market Singularities: The Strange Case of Bitcoin", *Journal of Cultural Economy*, vol. 10, pp. 462-473.
10. Demertzis, M., Wolf, G. (2018), "The Economic Potential and Risks of Crypto Assets: Is a Regulatory Framework Needed?", *Bruegel Policy Contribution*, issue n°14/2018.
11. EBA (2019), "Report with Advice for the European Commission on Crypto-Assets", 9 January 2019.
12. Edwards, F. and others (2019), "Crypto Assets Require Better Regulation: Statement of the Financial Economists Roundtable on Crypto Assets", *Financial Analysts Journal*, vol. 75, pp. 14-19.
13. ESMA (2019), "Initial Coin Offerings and Crypto-Assets", ESMA Advice, 9 January 2019.
14. European Commission (2018), "FinTech Action Plan: For a More Competitive and Innovative European Financial Sector", COM(2018) 109 final.
15. European Parliament (2020), Crypto Assets: Key Developments, Regulatory Concerns and Responses, Study requested by the ECON committee, PE 648.779, April 2020.
16. FATF (2014), "Virtual Currencies Key Definitions and Potential AML/CFT Risks", FATF, Paris.
17. FATF (2015), "Guidance for a Risk-Based Approach to Virtual Currencies", FATF, Paris.
18. FATF (2018a), "FATF Recommendations' Glossary" (as amended in 2018), FATF, Paris.
19. FATF (2018b), "Regulation of Virtual Assets", FATF, Paris.

20. FATF (2019), "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers", FATF, Paris.
21. Financial Stability Board (2018), "Chair's Letter to G20 Finance Ministers and Central Bank Governors", FSB, Basel.
22. FinCEN (2013), "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies", FinCEN Guidance.
23. FinCEN (2019a), "Advisory on Illicit Activity Involving Convertible Virtual Currency", May 9, 2019.
24. FinCEN (2019b), "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies", May 9, 2019.
25. Holman, D., Stettner, B. (2018), *Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches*, Allen & Overy, LLP.
26. Hughes, S. (2017), "Cryptocurrency Regulations and Enforcement in the U.S.", *Western State Law Review*, vol. 45, pp.1-28.
27. Irwin, A., Turner, A. (2018), "Illicit Bitcoin Transactions: Challenges in Getting to the Who, What, When and Where", *Journal of Money Laundering Control*, vol. 21, pp. 297-313.
28. Lagarde, C. (2018), "Addressing the Dark Side of the Crypto World", *IMF Blog*, 13 March 2018, available at: <https://blogs.imf.org/2018/03/13/addressing-the-dark-side-of-the-crypto-world/> accessed 14 April 2020.
29. Leaders of CFTC, FinCEN, and SEC Issue Joint Statement on Activities Involving Digital Assets
30. Low, K., Teo, E. (2017), "Bitcoins and Other Cryptocurrencies as Property?", *Law, Innovation and Technology*, vol. 9, pp. 235-268.
31. Massad, T. (2019), "It's Time to Strengthen the Regulation of Crypto-Assets", *Brookings Economic Studies Report,* Brookings Institution, Washington DC.
32. Maxson, S., Davis, S., Moulton, R. (2019), "UK Cryptoassets Taskforce Publishes its Final Report", *Journal of Investment Compliance*, vol. 20, pp. 28-33.
33. Mikhaylov, A., Frank, R. (2018), "Illicit Payments for Illicit Goods: Noncontact Drug Distribution on Russian Online Drug Marketplaces", *Global Crime*, vol. 19, pp. 146-170.
34. Miseviciute, J. (2018), "Blockchain and Virtual Currency Regulation in the EU", *Journal of Investment Compliance*, vol. 19, pp. 33-38.
35. Nair, D. (2019), "The Bitcoin Innovation, Crypto Currencies and the Leviathan", *Innovation and Development*, vol. 9, pp. 85-103.
36. Nance, M. (2018) "Re-thinking FATF: An Experimentalist Interpretation of the Financial Action Task Force", *Crime, Law and Social Change*, vol. 69, pp. 131–152.
37. Nolan, A., and others (2018), "Initial Coin Offerings: Key US Legal Considerations for ICO Investors and Sponsors", *Journal of Investment Compliance*, vol. 19, pp. 1-9.
38. Office of the New York Attorney General (2018), "Virtual Markets Integrity Initiative Report", New York.
39. Pavlidis, G. (2020), "Financial action task force and the fight against money laundering and the financing of terrorism: Quo vadimus?", *Journal of Financial Crime* [EarlyCite]

40. Reinicke, W. (1998), *Global Public Policy: Governing Without Government?*, Brookings Institution Press, Washington DC.
41. Rice, B. and Williams, B. (2019), "Cryptoassets Consumer Research Points to Ignorance and Risky Behaviour", *Journal of Investment Compliance*, vol. 20, no. 3, pp. 23-24.
42. Spafford, M., Stanaway, D. and Chung, S. (2019), "Blockchain and Cryptocurrencies: A Cross-Border Conundrum", *Journal of Investment Compliance*, vol. 20, no. 3, pp. 10-19.
43. Spithoven, A. (2019), "Theory and Reality of Cryptocurrency Governance", *Journal of Economic Issues*, vol. 53, pp. 385-393.
44. Stokes, R. (2012), "Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar", *Information & Communications Technology Law*, vol. 21, pp. 221-236.
45. Sveriges Riksbank, "E-krona Project: Report 1", Stockholm.
46. Swartz, L. (2018), "What Was Bitcoin, What Will It Be? The Techno-economic Imaginaries of a New Money Technology", *Cultural Studies*, vol. 32, pp. 623-650.
47. Teichmann, F. (2018) "Financing Terrorism Through Cryptocurrencies – A Danger for Europe?", *Journal of Money Laundering Control*, vol. 21, pp. 513-519.
48. TRACFIN (2019), "Tendance et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2017 et 2018", Traitement du renseignement et action contre les circuits financiers clandestins - TRACFIN, Paris.
49. Van Wegberg, R. and others (2018), "Bitcoin Money Laundering: Mixed Results? : An Explorative Study on Money Laundering of Cybercrime Proceeds Using Bitcoin", *Journal of Financial Crime*, vol. 25, pp. 419-435.
50. Vidal-Tomas, D., Ibanez, A., Farinos, J. (2019), "Weak Efficiency of the Cryptocurrency Market: A Market Portfolio Approach", *Applied Economics Letters,* vol. 26, pp. 1627-1633.
51. Whyte, C. (2020), "Cryptoterrorism: Assessing the Utility of Blockchain Technologies for Terrorist Enterprise", *Studies in Conflict & Terrorism* [latest articles].
52. Wong, M. (2019), "Hong Kong Regulation of Crypto-Related Investments", *Journal of Investment Compliance*, vol. 20, no. 4, pp. 45-50.
53. Yanagawa, N., Yamaoka, H. (2019), "Digital Innovation, Data Revolution and Central Bank Digital Currency", *Bank of Japan Working Papers*, No.19-E-2.
54. Zilioli, C. (2020), "Crypto-Assets: Legal Characterisation and Challenges under Private Law", *European Law Review*, vol. 46, pp. 251-266.