CHALLENGES OF THE USE OF VIRTUAL ASSETS IN MONEY LAUNDERING

VICTORIA KOUTSOUPIA*

Cryptocurrencies have vast potential, but they also present significant risks related to money laundering and terrorist financing due to their technical characteristics. Crypto-assets are essentially applications of blockchain technology, which entails a public, encrypted, and secure ledger distributed across a network of validated computers. Each computer operates with common software that fosters consensus on new entries and prevents unauthorized alterations to the agreed-upon register. The Financial Action Task Force (FATF) has issued numerous guidelines on virtual assets, and in September 2020, the European Commission embraced the Digital Finance Package to bring the EU in line with the digital age. A pivotal component of this package is Regulation (EU) 2023/1114 of the European Parliament and of the Council, dated May 31, 2023, on markets in crypto-assets, known as MiCA Regulation. This regulation signifies the EU's endeavor to standardize the legal framework for crypto assets while actively contributing to the prevention of money laundering and terrorist financing. The challenge for regulatory authorities lies in the seizure, confiscation, and forfeiture of crypto-assets as proceeds of crime, given their inherent characteristics that impede traceability. Court decisions outlined in this article underscore the difficulties faced by law enforcement authorities when handling crypto-assets as proceeds of crime. The article examines how European legal authorities and the FATF utilize various legal tools, such as Directives, Regulations, and Guidelines, to adapt to the evolving landscape of virtual assets. To mitigate the risk of forum shopping, where individuals seek the most favorable legal regime, alignment of the legal frameworks of Member States is crucial. The ongoing evolution of the legal framework reflects the persistent challenges posed by virtual assets in the context of criminal activities, prompting a continuous adaptation of regulations by European legal authorities and the FATF.

1 THE DEVELOPMENT AND PROLIFERATION OF VIRTUAL ASSETS

Crypto-assets or virtual assets constitute only a small part of the international financial system, including payment schemes, but they have unlimited potential for further development. Virtual assets represent more than just the digitization of money; they are a way to rebuild trust,[1] a pioneering response to the erosion of trust in the banking system that

* Post Doctoral Researcher in Criminal Law, University of Cyprus (UCY). Legal Representative of the Legal Council of the Hellenic State.

[1] Laura Shin, 'Why Wall Street Journal Currency Report Didn't Understand Money Until He Learned About Bitcoin' (*Forbes*, 20 September 2016) <https://www.forbes.com/sites/laurashin/2016/09/20/why-a-wall-street-journal-currency-reporter-didnt-understand-money-until-he-learned-about-bitcoin/?sh=30f63c744c4e> accessed 10 December 2023; Paul Vigna and Michael J Casey, *Cryptocurrency – how bitcoin and Digital Money are Challenging the Global Economic Order* (St. Martin's Publishing Group 2015) 38.

unfolded since the onset of the economic crisis in 2007.[2] Decentralized crypto-assets, such as Bitcoin and similar virtual assets, are gaining ground globally in the financial world as they represent the most innovative form of payment. In recent years, they have often been associated with criminal activities.[3] The fact that crypto-assets facilitate criminal activities is not new and is widely known.[4] It is observed that criminals use them to anonymize and transfer ill-gotten assets in an untraceable manner. It is noteworthy that nearly half of all Bitcoin transactions can be linked to illegal activities, according to Australian researchers who used specific algorithms to analyze transaction information. Justifiably, there is concern about the growing use of cryptocurrency assets in relation to financial crime.

Crypto-assets undoubtedly are gateways for money laundering and terrorist financing, which criminals can easily exploit. The fact that they are entirely digitalized assets, easily transferable, with no requirement for true identification information – thus with a certain level of anonymity – and the ability to operate on a decentralized basis, makes them particularly conducive to money laundering and other criminal activities.[5]

Virtual assets pose a significant challenge for both national and international legislators, as it has become evident in the approximately fifteen-year history of Bitcoin. Their technical characteristics and peculiarities make it difficult to address them in traditional regulations. However, the most intricate issue is regulating virtual assets within the framework of combating money laundering and terrorist financing and effectively confiscating them in cases where they are products of crime.[6]

Due to the technical nature of digital currencies, the terminology used might be confusing. To clarify, while digital currencies constitute a broad phenomenon, terminology often associates cryptocurrencies with Bitcoin, which is simply the most well-known example.[7] Reference is often made to Bitcoin, and most conclusions related to this currency will be similar or identical to other cryptocurrencies and crypto-assets. Article 3(1) para 5 of the MiCA Regulation[8] defines crypto-assets as a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology.

---

[2] James Crotty, 'Structural causes of the global financial crisis: A critical assessment of the new "financial architecture"' (2009) 33(4) Cambridge Journal of Economics 563, 565.

[3] Jacek Czarnecki, 'Digital Currencies and the Anti-money Laundering/Counter- terrorism Financing Regulations in the EU: Imaginary Risk or Real Challenge?' in Katalin Ligeti and Michele Simonato (eds), *Chasing Criminal Money, Challenges and perspectives on asset recovery in the EU* (Hart Publishing 2017) 287.

[4] Fabian Maximilian Johannes Teichmann and Marie-Christin Falker, *Cryptocurrencies and financial crime: solutions from Lichtenstein* (2021) 24(4) Journal of Money Laundering Control 775.

[5] Robby Houben and Alexander Snyers, 'Crypto-assets: Key Developments, Regulatory Concerns and Responses' (2020) Study Requested by ECON committee, 10 <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf> accessed 10 December 2023.

[6] Czarnecki (n 3) 287.

[7] European Central Bank, 'Virtual Currency Schemes' (2012) <www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> accessed 10 December 2023; European Central Bank, 'Virtual Currency Schemes- A Further Analysis' (2015) <www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> accessed 10 December 2023; Financial Action Task Force (FATF), 'Virtual Currencies: Key Definitions and Potential AML/CFT Risks' (2014) FATF Report <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 10 December 2023.

[8] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 [2023] OJ L150/40 (MiCA Regulation).

It is practically impossible to provide a comprehensive description of the technological and economic aspects of crypto-assets or the technology on which they are built and therefore will not be the aim of this article. However, some peculiarities of Bitcoin, and crypto-assets in general, are important to mention within the context of applying legislation to combat money laundering in various activities related to cryptocurrencies. Moreover, to understand how the confiscation of crypto-assets as proceeds of criminal activities can be made possible, the characteristics of this type of currency should first be described.

Crypto-assets are built on a technology called 'blockchain'.[9] At its most fundamental level, blockchain is a public, distributed ledger that cannot be altered. The ledger is not stored by a central entity but is distributed among multiple nodes in the network, making it decentralized. The innovation behind blockchain technology (often referred to more broadly as 'distributed ledger technology' or 'DLT') is that it allows identical forms of the ledger to be maintained by nodes, even though each node is unable to impose its own form on others. This is achieved through the use of cryptographic solutions, which assist in reaching consensus among the nodes about which form of the ledger is valid.

In the case of Bitcoin, which represents the first, and so far the most successful, application of this technology, the issuance of currency is allowed without a central issuer, and, as a result, it is not subject to involvement and manipulation by governments.[10] Transactions within a network without intermediaries, such as banks, are also possible. The operations of the blockchain exist as a record of all transactions that have occurred on the blockchain network and are maintained by a series of nodes distributed worldwide. One peculiarity of blockchain technology is that no single entity is solely responsible for the maintenance and control of the blockchain network.

2 CRYPTO-ASSETS AND THE DEVELOPMENT OF BLOCKCHAIN TECHNOLOGY

It is important to emphasize that crypto-assets do not constitute a separate capital of financial innovation but have created significant opportunities in this sector. Bitcoins were simply the first application of blockchain technology. A blockchain technology is a public, encrypted, and secure ledger distributed across a network of validated computers, each of which operates with common software that leads to consensus on new entries and prevents unilateral reentries into the agreed-upon register.[11] Blockchain technology allows for the creation of different asset elements (cryptographic assets) that represent value, existing without any central intermediary. For example, units in a blockchain may be treated not as currency but as shares in a company or other types of rights. Furthermore, the use of smart contracts, i.e. immutable and self-executing contracts executed in a specific blockchain, in certain blockchains, such as Ethereum, enables the creation of complex collaborative structures which operate without central administration.

[9] Certainly, a distinction should be made between the reference to 'blockchain' and 'Blockchain', as the latter specifically refers to the database used in Bitcoin, while the former is a more general term that encompasses the technology itself.
[10] Andrew Haynes and Peter Yeoh, *Cryptocurrencies and Cryptoassets: Regulatory and Legal Issues* (Routledge 2020) 7.
[11] Vigna and Casey (n 1) 64.

There are two main consequences arising from the above, with a focus on regulatory strategies to combat money laundering and terrorist financing. First and foremost, legislators and regulatory authorities should be aware that currency is just one out of many possible applications of blockchain technology. Next-generation applications already include other forms of value. These are based on similar technology but may have different social applications and economic significance. Secondly, new developments, such as decentralized autonomous organizations, introduce an entirely new level of complexity. Cryptocurrencies may require an immediate regulatory response, but regulatory authorities should not overlook further blockchain technologies.[12]

3 THE USE OF CRYPTO-ASSETS FOR MONEY LAUNDERING AND TERRORISM FINANCING

The use of crypto-assets as tools for money laundering and terrorism financing has garnered the interest of many public authorities and organizations, including Interpol and Europol. The latter has described crypto-assets as one of the key drivers changing the way serious and organized crime operates: 'Virtual currencies gradually enable individuals to act as free criminal entrepreneurs conducting crime as a service business model, without the need for advanced criminal infrastructure for money receipt and laundering'.[13] Crypto-assets have been characterized as the ideal tool for money laundering. The assertion that digital currencies enhance the risk of terrorism financing was also supported in the FATF's relevant report titled 'Emerging Terrorist Financing Risks' issued in 2015.[14] Furthermore, Europol stated in the '2015 Internet Organized Crime Threat Assessment' that 'Bitcoin is establishing itself as the single currency for criminals operating in the cybercrime space within the EU' and proposes 'harmonized legislative changes at the European level or the unified application of existing legal tools, such as regulations for combating money laundering, to address the criminal use of virtual currencies'.[15] Interpol even created its own cryptocurrency to learn more about how criminal activities involving digital currencies can be fought. Interpol and Europol have also established a partnership 'against the abuse of virtual currencies for criminal transactions and money laundering', which includes 'policy actions, strengthening cooperation and development programs, and delivering training to combat the criminal use of virtual currencies, allowing for the detection, confiscation, and forfeiture of criminal assets'.[16]

---

[12] Czarnecki (n 3) 291.

[13] European Police Office (Europol), 'Exploring Tomorrow's Organized Crime' (2015), 9, 30 <https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_OrgCrimeReport_web-final.pdf> accessed 10 December 2023.

[14] FATF, 'Emerging Terrorist Financing Risks' (2015) FATF Report, 24 <https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf> accessed 10 December 2023.

[15] Interpol, 'Darknet Training Shines Light on Underground Criminal Activities' (*Interpol*, 31 July 2015)<https://www.interpol.int/News-and-Events/News/2015/INTERPOL-Darknet-training-shines-light-on-underground-criminal-activities> accessed 10 December 2023.

[16] Europol, 'Europol - Interpol Cybercrime Conference Makes the Case for Greater Multisector Cooperation' (*Europol*, 2 October 2015) <https://www.europol.europa.eu/media-press/newsroom/news/europol-%E2%80%93-interpol-cybercrime-conference-makes-case-for-greater-multisector-cooperation> accessed 10 December 2023.

There is a need for continuous, evidence-based, and in-depth empirical analysis of the use of virtual assets for illegal activities. It is not unlikely that new evidence or arguments regarding the use of virtual assets for money laundering and terrorism financing triggered and expedited regulatory proposals in the EU concerning the combat against money laundering and terrorism financing.[17]

The constantly emerging challenges in the field of crypto-assets regarding money laundering have led to the publication by the FATF in June 2022 of the 'Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs'.[18] Only a year later on June 2023, FATF published another update regarding virtual assets under the title: 'Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers'.[19] The last report is an update on country compliance with FATF's Recommendation 15 and its Interpretative Note (R.15/INR.15), including the Travel Rule, and updates on emerging risks and market developments, including on Decentralized Finance (DeFi), Peer-to-Peer transactions (P2P), and Non-Fungible Tokens (NFTs), unhosted wallets, and stablecoins.

The European Commission adopted the Digital Finance Package in September 2020, in order to respond to the challenges of the digital age. The package includes the digital finance strategy, retail payments strategy, crypto-asset legislative proposals, and digital operational resilience legislative proposals. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, which is also known as MiCA Regulation, is based on Article 114 TFEU, which lays the legal groundwork for establishing an internal market. The EU is empowered to enact legislation harmonizing any national laws that might hinder the free movement of goods, services, capital, or people, thereby addressing obstacles to the internal market. The MiCA Regulation has been proposed following the subsidiarity principle, which allows the Union to intervene and take action when the objectives of an action cannot be adequately achieved by the Member States on their own.

The EBA and ESMA have previously emphasized that, despite existing EU legislation specifically addressing money laundering and terrorism financing, a majority of crypto-assets remain beyond the purview of EU financial services regulations. Consequently, they escape provisions related to consumer and investor protection, market integrity, and similar aspects, despite carrying associated risks.

In light of this, the MiCA Regulation aims to actively contribute to the prevention of money laundering and terrorism financing. In this context, it is imperative that the definition of 'crypto-assets' aligns with the one outlined for 'virtual assets' in the recommendations of the FATF. Moreover, any catalog of crypto-asset services should encompass virtual asset

[17] Czarnecki (n 3) 291.

[18] FATF, 'Targeted Update on Implementation of FATF Standards on Virtual Assets and Virtual Asset Service Providers' (2022) <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf.coredownload.pdf> accessed 10 December 2023.

[19] FATF, 'Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers' (2023) <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/June2023-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf> accessed 10 December 2023.

services that are likely to raise concerns related to money laundering, as identified by the FATF.[20]

4 CONFISCATION OF CRYPTOCURRENCIES

The unique nature of crypto-assets poses many challenges regarding the effective detection, investigation, and confiscation of proceeds of crime related to them.[21] Specifically, the inadequate knowledge about virtual assets, their characteristics, and the techniques that could be used to combat crypto-assets related with criminal activities make their detection more difficult. Their digital nature mainly entails electronic evidence of the crimes committed, encumbering the addressing of crimes involving them. Furthermore, there is often a lack of legislative and regulatory responses specifically aimed at recovering proceeds of crime acquired through or with the assistance of virtual assets. Additionally, difficulties in monitoring and coordinating actions taken, both at national and international levels, have been identified.[22]

To consider the conversion of assets into crypto-assets or vice versa as a criminal offense, it must first be assessed whether and to what extent crypto-assets can be considered assets, assigning them the appropriate legal classification.[23] Depending on such classification, it can then be determined how and whether the confiscation of these crypto-assets is possible. According to case C-264/14[24] and in accordance with the 2012 report of the European Central Bank, virtual currencies were defined as electronically transmitted money, not subject to regulation. The issuance and control of these funds by their issuers are accepted by their members. Some similarities exist between these virtual currencies and other exchangeable currencies in terms of their use. However, there are significant differences, as they cannot be expressed in any conventional unit, such as euros or dollars, but in a virtual unit (for example bitcoin). Therefore, the Court's judgment was that bitcoin constitutes a conventional means of payment and could therefore be characterized as an intangible asset.[25] Directive 2018/843/EU defines virtual assets as digital representations of value that are not issued by a central bank or public authority. They do not have their guarantee, are not necessarily linked to legally circulating currencies, and do not have the legal status of currency or money, but are accepted by natural or legal persons as a means of exchange and can be transferred, stored, or electronically traded.[26]

---

[20] Commission, 'Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937' COM (2020) 593 final, 4.

[21] United Nations Office on Drugs and Crime (UNODC), 'Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies' (2014) <https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf> accessed 10 December 2023.

[22] Czarnecki (n 3) 291.

[23] George Papadimitrakis, 'Legitimization of Income from Criminal Organization and Cryptocurrencies' (2018) 9 Armenopoulos 1598.

[24] Case C-264/14 *Skatteverket v David Hedqvist* EU:C:2015:718.

[25] For the current regulations in the USA, see Christos Mylonopoulos, 'Is issuance possible in the USA for legitimizing cryptocurrencies derived from criminal activity' (2018) Criminal Chronicles 185; Texas District Court's decision, SEC v Shavers, 2013 Fed. Sec. L. Rep, CCH) P 97, 596 (E.D. Tex Aug 6, 2013) Jeffrey E. Alberts & Bertrand Fry Is B A Security/ BITCOIN J. Sci. & Tech.

[26] 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

Confiscation, forfeiture or seizure of the proceeds or instruments of crime are complex processes, both substantively and procedurally. Naturally, their application to virtual assets is even more complex due to their particular characteristics (anonymity, difficulty of traceability, possibility of cross-border transactions).[27] Transactions involving crypto-assets are not recorded. They are anonymous, international, and irreversible. When traditional legal tools of criminal prosecution and enforcement are applied in cases involving decentralized virtual currencies, challenges arise. For example, there might not be a contracting party, such as a central administrator, who can identify and apply attachment and confiscation decisions to assets held in the form of crypto-assets. Under these circumstances, it becomes difficult for regulatory authorities to take enforcement actions involving the seizure, forfeiture, and confiscation of illegal assets. FATF guidelines provide some guidance on clarifying responses to money laundering risks arising from crypto-assets, but each national jurisdiction has adopted a different approach to regulating on the matter.[28]

The provided anonymity impedes determining the individuals involved. The protocols on which almost all decentralized crypto-assets are based do not require identification and verification of participants. Moreover, the transaction history records created on the blockchain from the basic protocols are not necessarily linked to the real-world identity of the person. This level of anonymity restricts the usefulness of the blockchain for monitoring transactions and detecting suspicious activity. It poses a significant challenge for law enforcement authorities to trace illegally obtained income that may be laundered using cryptocurrencies, let alone confiscate them. Additionally, these authorities cannot target a central location or entity for investigative purposes.[29]

Furthermore, there is an additional risk of not being able to locate the legal entity responsible because virtual currencies do not require the involvement of a third party, with the possible exception of exchanges. Consequently, criminal prosecution cannot be pursued, and therefore, the confiscation of the proceeds of crime cannot be imposed. Senders and recipients can conduct transactions with cryptocurrencies directly, without requiring identification, as there are no names attached to wallet addresses, and there is no mediation that could involve informing authorities of suspicious transactions. Crypto-assets as payment methods are not limited and are accepted without jurisdictional boundaries. Crypto-assets transactions require nothing more than internet access, and their infrastructure is often distributed worldwide hindering tracing irreversible transactions. In addition, crypto-assets operate and evolve online, blurring national borders and elevating e-commerce to an international phenomenon. In light of these facts, one of the most challenging aspects of recovering the proceeds of crime in cases related to virtual assets is the applicable jurisdiction and the requirements for international cooperation.[30]

Beyond the above, another factor that discommodes confiscation of crypto-assets is the fact that no interaction with the regulated financial system is required, and transactions

terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L156/43 (Directive 2018/843) Art 1(2)(d).

[27] UNODC, 'Basic Manual' (n 21) Module 4: Seizure of Virtual Currencies, 135.

[28] Haynes and Yeoh (n 10) 16.

[29] FATF, 'Guidance for a Risk-based Approach to Virtual Currencies' (2015) 38 <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-RBA-Virtual-Currencies.pdf.coredownload.pdf> accessed 10 December 2023.

[30] UNODC, 'Basic Manual' (n 21) Module 4: Seizure of Virtual Currencies, 135.

are not monitored. Moreover, piracy in crypto-assets software, wallets, and exchanges, allow criminal organizations to involve other individuals in their illegal activities. It is a fact that criminals tend to use any available means to cover their tracks. There are no adequate safeguards to combat piracy and there is a lack of controls on electronic wallet providers, exchanges, and trading platforms. This allows criminals to steal identities and consequently involve others in their criminal activities. In this way, in some jurisdictions, the seizure of assets and confiscation is avoided.[31] Specifically regarding confiscation, in cases where asset forfeiture procedures are correctly applied, the confiscation of crypto-assets or their equivalent value should not significantly differ from the confiscation of other forms of property.

Recently, the United Nations Office on Drugs and Crime issued the 'Digest of Cyber Organized Crime,[32] resolving some issues arising from the use of crypto-assets in criminal activities, such as jurisdiction, identification, and tracing of illegal assets. However, in practice, the problem remains that the use of cryptocurrencies by criminals makes it nearly impossible to achieve restorative justice for the victims, as the seizure and confiscation of the proceeds of crime is neither easy nor speedy.[33]

Regulatory rules regarding the confiscation of criminal proceeds, both at national and international level, appear inadequate in addressing the challenges associated with crypto-assets. There are no established practices for recovering criminal proceeds at any of the usual stages: detection, seizure, and confiscation of digital currencies. The Directive adopted on the confiscation and recovery of crime proceeds establishes a framework of minimum rules imposed for the detection, tracing, and confiscation of the proceeds of crime throughout the EU[34] and represents a step in the right direction. However, it raises the question of whether national legislation regarding the application of the Directive will be effectively applied in cases involving cryptocurrencies.[35]

It should be noted that there have been few cases involving the seizure and confiscation of virtual assets on an international level. Therefore, much of what is discussed below is based on general principles of establishing jurisdiction over virtual currencies as products/tools of crime.[36] One of the biggest challenges here is the so-called 'cloud computing'. Virtual assets wallets are stored in a 'cloud' infrastructure and are subject to frequent data transfers from one server to another, easily bypassing national borders. In cybercrime investigations facing such challenges, this is often referred to as 'location loss'. However, the principle of territoriality remains the starting point for establishing jurisdiction. Therefore, all means of cooperation should be used to attempt to determine the location of a wallet for as long as the data remains in a specific server within a particular jurisdiction.[37]

---

[31] European Banking Authority, 'Opinion on "Virtual Currencies"' EBA/Op/2014/08, 33.
[32] UNODC, 'Digest of Cyber Organized Crime' (2022) 108 <https://sherloc.unodc.org/cld/uploads/pdf/22-10875E_ebook_cb.pdf> accessed 10 December 2023.
[33] European Banking Authority, 'Opinion on "Virtual Currencies"' (n 31) 33.
[34] Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union [2014] OJ L127/39.
[35] Czarnecki (n 3) 293.
[36] UNODC, 'Basic Manual' (n 21) Module 4: Seizure of Virtual Currencies, 135.
[37] Jan Spoenle, 'Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?' (2010) Discussion Paper prepared for the Economic Crime Division of the Council of Europe, 5 <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3df> accessed 10 December 2023.

Financial investigations focusing on virtual currencies as products and tools of crime are relatively recent. Therefore, tested approaches addressing issues arising from the use of virtual assets[38] have not yet been developed. The identification of assets and, in general, the tracking of the money's path are crucial parts of financial investigations in order to establish the criminal origin of the products or to determine the means of the crime. The identification of assets, as in any criminal or financial information investigation, relies on certain indicators, known as 'red flags', which can assist and guide the investigator in determining the criminal nature of the assets under scrutiny. This method of identification is useful not only for investigations but also for tracking virtual currency transactions.

As indicators, red flags are considered:

a) A large number of bank accounts maintained by the same administrator of a virtual assets exchange company, sometimes in different countries, used as accounts for continuous money flows (it may be an indicator of layering, which constitutes the second stage of money laundering), without any logical reason for such a structure;
b) The existence of a virtual assets administrator or exchange company based in one country but having accounts in other countries without a significant customer base in the latter, indicating an inexplicable business policy that may be considered suspicious;
c) Capital transfers between bank accounts maintained by different administrators of virtual assets exchange companies domiciled in different countries, which again may constitute an indicator of layering if it does not align with a business model;
d) The intensity and frequency of cash transactions structured in a way that does not exceed the reporting threshold conducted by the owner of a virtual assets' administrator or virtual currency exchange company without any economic sense or purpose;
e) Virtual assets systems lacking proper registration and transparency are popular among criminal groups.

As it is evident from the above, these indicators are directed at the points of contact between crypto-assets and established institutions, currency exchanges, payment services for virtual assets, and hosting services.

In the event that, despite the aforementioned challenges, the confiscation and seizure of crypto-assets as proceeds of crime are achieved, law enforcement agencies face the challenge of managing the seized assets. The ownership of the property remains with the original owner as long as the confiscation decision is pending, and for this reason, the management of the seized assets should be handled with great care. Virtual assets, whether centralized or decentralized, cannot undergo physical deterioration as crypto-assets,[39] although they are subject to significant fluctuations in exchange rates. This may concern law enforcement authorities as the confiscation of assets may be pending. The value of the

[38] UNODC, 'Basic Manual' (n 21) Module 4: Seizure of Virtual Currencies, 135.
[39] David Gilson, 'Bitcoins seized by Drug Enforcement Agency' (*CoinDesk*, 24 June 2013) <http://www.coindesk.com/bitcoins-seized-by-drug-enforcement-agency/> accessed 10 December 2023.

confiscated property at the time of discovery and during the final confiscation might vary significantly. Therefore, a revision of the amount and value of the cryptocurrencies to be seized may be required.[40]

5 JUDICIAL DECISIONS REGARDING CONFISCATION OF CRYPTOCURRENCIES

Given the unique nature of crypto-assets, there have been few judicial decisions ordering confiscation as mentioned above. One of the few decisions addressing this issue is the discussed below decision of the German Federal Court (Bundesgerichtshof – BGH), which could open to a fruitful dialogue on how to address the significant challenges that arise. This study aims to highlight the complexity of judicial control in light of the use of advanced technological methods by criminals, which appear to outpace law enforcement authorities. However, the primary problem that needs to be stressed for further consideration is the significant difficulty in actually removing criminal proceeds or assets when they are virtual assets stored with a private key known only to the owner. There is a significant risk that the perpetrator of the crime is sentenced to a term of imprisonment but still retains an unchanged, if not significantly larger – due to fluctuations in the value of crypto assets – criminal wealth acquired from the crime.

This article aims to shed light on certain of these aspects and highlight issues in the context of the transnational and international confiscation of cryptocurrencies. Specifically, according to the facts described in the decision No. 1 StR 412/16 of July 27, 2017 by the German Federal Court, two perpetrators jointly decided in early 2012 to organize a botnet. The said botnet consists of a union of a large number of computers where programs automatically perform repetitive computational tasks in the background, without the user's knowledge. These programs automatically connect to a central command and control server called a bot herder, allowing remote control of the connected computers, with the aim of benefiting the individuals who control the central server. The botnet designed by the perpetrators was aimed both at Bitcoin mining and data espionage. Victims unknowingly installed bots on their computers through what is known as a 'Trojan horse', a camouflaged malicious software. Additionally, victims' computers were infected through a security vulnerability in their operating system, web browser, or some software.

Bitcoin is a globally available decentralized payment network and a virtual assets unit. Bitcoins are transferred over the internet and processed through a decentralized network of computers, without the involvement of a central authority. The management of these funds is entrusted to individual participants through personal digital wallets. For this purpose, there is a public key that is recognizable to every network participant and a private key known only to the wallet owner. The market value of Bitcoin is determined by supply and demand. Each transaction must be confirmed as valid by the majority of participants in the network to be considered completed. Subsequently, this results in the simultaneous creation of new Bitcoins. The computational operations required to verify transactions involve solving cryptographic tasks that extend the public transaction ledger of the cryptocurrency (blockchain). The algorithms that need to be solved become increasingly complex as the

[40] UNODC, 'Basic Manual' (n 21) Module 4: Seizure of Virtual Currencies, 135.

number of Bitcoins increases. At the same time, the total computational power required to solve them also increases. Each participant who performs the computational task is rewarded with the recently mined Bitcoins in their digital wallet. As the computational power increases, the likelihood of finding the correct result also increases. However, the cost of electricity required by regular processors minimizes the profitability derived from the newly created Bitcoins. To increase their value, the bot herder, who controls the botnet network through the central command and control server, engages in illegal activities. The perpetrator burdens unsuspecting computer users with the cost of electricity consumption during the resolution of computational tasks, which he has already infected with malicious software.

According to the actual circumstances of the decision, one of the two perpetrators created a 'Trojan horse' in the form of music, video, or a program offered for download from the internet. In this way, he gained the ability to mine Bitcoin through the computers of unsuspecting users, burdening them with the cost of electricity consumption. Subsequently, the two perpetrators jointly enriched the malicious software with a concealment wall developed by one of them with the main malicious software program. One of the two defendants then began uploading files infected with malicious software to various Usenet servers. The Trojan horse was intended for operating systems from Windows XP to Windows 7. The firewall serves as access protection for networks and is configured to prevent attacks on the user's computer from the internet. If the malicious software that the user had downloaded did not take the form of music, video, or a program, the program that allowed the central command and control server to access the computer would have undergone this check through the firewall, and access would have been denied.

From early 2012 until the end of the following year, 327,379 users unknowingly 'downloaded' malicious software onto their computers, believing it to be a desired music, video, or program file. When asked if they wanted to install the program, they responded affirmatively, thereby unintentionally installing the Trojan horse on their computers, and disabling their Firewall protection programs in at least 245,534 cases during the execution of this act. This action allowed the perpetrators to gain access to the users' data. The users believed they were downloading harmless files, while in reality, they were unwittingly installing spyware and granting access to their network data. Without this deception of the users, access to the data would have been prevented by the Firewall program, which would have rejected incoming connection requests from the network controlled by the defendants. After 120 seconds of user inactivity, the computing power of the computers' graphics cards was used to perform complex calculations, for which the perpetrators were rewarded with Bitcoin crypto-assets. Furthermore, through another program (Zeus), the registration of user account information, secret numbers, and passwords was transferred to the defendants in an unencrypted format.

According to Article 303a of the German Criminal Code, anyone who unlawfully deletes, copies, renders useless, or alters data is punishable by law. This provision protects the interest of the holder in the integrity of stored or transmitted data. In this regard, it was found that the legal requirements of provision were satisfied as the installation of malicious software changed the settings' content to execute certain functions. Data alteration, as mentioned in the objective substance of Article 303a of the German Criminal Code, is established by impairing the function of the data, resulting in a change in their informational

content.[41] Furthermore, according to Article 303a of the German Criminal Code, anyone who, without authorization, gains access to data not intended for them and protected against unauthorized access is punishable by law. Data are considered protected when the holder has declared interest in maintaining confidentiality by taking security measures.[42] In the present case, the data was highly protected against unauthorized access through the activated Firewall system. Therefore, the defendants, by gaining access to the data, essentially committed the crime described in Article 303a of the German Criminal Code.

There is a plurality of crimes, the value of which can be captured and attributed through the application of multiple criminal provisions.[43] According to the considerations in the discussed decision, the aforementioned actions are committed together in fact. In general, this happens when multiple crimes are committed through a single act.[44] It is generally considered that crimes are committed together when one crime is committed during the commission of a continuous crime and until the completion of this crime.[45] In this case, the actions were committed in a factually consecutive manner according to Article 25 para. 1 of the German Criminal Code since the victims themselves unintentionally installed the Trojan horse on their computers.[46]

According to Article 73 para. 1 of the German Criminal Code, as it stood before the amendment on 1 July 2017, if a punishable act was committed, and the perpetrator or participant has gained anything from it or for it, the court would order its forfeiture. This provision does not apply in cases where the victim has a gain, the satisfaction of which would remove the value of what has been acquired from the act of the perpetrator or the participant. In its current form of the article, it is provided that if the perpetrator or participant has acquired anything from the punishable act or for it, the court orders its seizure.

As it emerges from the above facts of the case, Bitcoin, regardless of their legal nature, were acquired through a criminal act, specifically through the alteration of data under Article 303a of the German Criminal Code. In light of their market value, they constitute a realizable economic value, given that the defendants were the beneficiaries with the right to dispose of them.[47] Therefore, their confiscation was ordered under Article 73(1) para. 1 of the German Criminal Code, in its previous formulation. The argument that Bitcoins cannot be confiscated because they do not constitute an object, or a right, cannot be accepted. Due to their inclusion in a Blockchain network and the combination of the public and the defendant's known private key, they were adequately determined. Consequently, they can be confiscated, even if they are not tangible objects. However, the notion in the decision, that whether the defendant's private key for the digital wallet is known to the investigative

[41] Deutscher Bundestag 10. Wahlperiode (1986) Drucksache 10/5058, 35; Sonja Heine, 'Bitcoins und Botnetze – Strafbarkeit und Vermögensabschöpfung bei illegalem Bitcoin-Mining' (2016) NStZ 441-443.
[42] BGH cases dated at 21st July 2015 – 1 StR 16/15, NStZ 2016, 339, on 6th July 2010 – 4 StR 555/09, NStZ 2011, 154, Graf/Jäger/ Wittig, (2017), Wirtschafts- und Steuerstrafrecht Kommentar, 2nd edition, article 202a, no. 19, C.H. Beck.
[43] Heinz-Bernd Wabnitz and Thomas Janovsky, *Handbuch des Wirtschafts und Steuerstrafrechts* (4th edn, C.H. Beck 2014) 14th chapter, no 108; Thomas Fischer, *Strafgesefzbuch* (64th edn, C.H. Beck 2017) article 303a, no 2; Hagen Wolff et al, *Strafgesetzbuch. Leipziger Kommentar* (12th edn, De Gruyter 2008) article 303a no: 4, 798.
[44] Christos Mylonopoulos, *Criminal Law, General Part* (P.N. Sakkoulas 2008) Chapter II, 324.
[45] Stamati, *Systemic Interpretation of Criminal Law* (P.N. Sakkoulas 2005) Articles 1-133, Article 94 n. 35, 986.
[46] Thomas Frank, in Eric Hilgendorf et al, *Informationsstrafrecht Und Rechtsinformatik* (Logos Berlin 2004) 23.
[47] BGH, case of 12th May 2009 – 4 StR 102/09, NStZ-RR 2009, 320, and of 17th of March 2016 – 1 StR 628/15, BGHR StGB article 73.

authorities does not affect the confiscation provision, is problematic. The decision was based on the fact that knowledge of the key is not a prerequisite for the effective assumption of the power of disposal over the Bitcoins, as it concerns only the execution of the provision and does not affect the provision per se. The court overlooked that the private key was not known at the time of the provision's issuance, and the cooperation of the defendants in its execution was absolutely necessary, without, however, being able to compel them to cooperate.

In this way, the judicial decision persists in a sphere of legal formalism, bypassing the fundamental problem of cases of this nature, namely the confiscation of criminal wealth acquired in Bitcoins, which requires knowledge of the private key of the perpetrators. The retention of criminal wealth sends the message that crime 'pays' and, given that organized criminal groups are significantly affected only when they are deprived of their profits, while they are hardly affected by the imposition of a penalty on a member,[48] the risk of the use of advanced technological means for the commission of crimes looms large.

The analysis of the above decision raises several issues. Firstly, due to the complex structure and operation of such criminal activities, which are carried out exclusively through the use of technology, their investigation proves to be extremely challenging, especially in locating and quantifying criminal proceeds. Furthermore, the primary issue appears to be the existence of a private key that prevents authorities from accessing the digital wallets of the defendants even after confiscation. Therefore, in cases where the defendant does not disclose their private key, it is highly likely that they will retain their criminal gains. Exceptional difficulty also arises in determining the victim's damages, to the extent that the claim for restitution loses substance. Moreover, competent authorities require appropriate training, sufficient staffing, and the necessary resources to effectively combat criminal activities in the digital sphere. The use of crypto-assets for criminal purposes obliges the European legislator to continuously update legislation to align with current realities.

Another case from the Bulgarian court regarding the seizure of crypto-assets worth 3,000,000,000 bitcoins is also discussed. More specifically, Bulgarian law enforcement authorities, in cooperation with the Southeast European Law Enforcement Center, a local organization consisting of 12 Member States based in Bulgaria, conducted a coordinated effort in May 2017 to dismantle an extremely complex criminal organization. In this successful operation, authorities arrested 23 Bulgarian nationals and seized 213,519 bitcoins. The criminal organization's modus operandi involved sophisticated techniques, including piracy within the Bulgarian customs department, to ensure that the associates of the criminal organization did not pay the required duties for importing products into the country. To execute their plan, the criminal organization had installed viruses in electronic systems through corrupt customs officials to allow remote access to hackers. In this way, it appeared that the duties for the cargoes of the criminal organization's associates were paid, while, in reality, the obligation to pay still existed. As a result, for the year 2015 alone, approximately 5,000,000 Euros in damages were incurred by the customs department. During the investigation, law enforcement authorities seized 213,519 bitcoins, valued at 500,000,000

[48]Aristomenis Tzannetis, 'The confiscation of laundered products of criminal activity' in Minutes of the 4th Congress of the Hellenic Criminal Bar Association: Money laundering – 'Clean or Free Society?' [in Greek] (2007) 249.

dollars at the time. With the inflation of the Bitcoin's value from the time of confiscation until December 2017, the seized amount had reached 4,000,000,000 dollars. The criminal organization chose to use Bitcoins due to their capacity of evading authorities' control. The seizure of such a significant amount of crypto-assets could serve the purpose of bolstering the state budget.

It should be noted that there is lack of specialized knowledge among law enforcement authorities regarding the operation of crypto-assets. Therefore, there is a risk of a significant decrease in the value of the seized assets. In the case discussed above, the value of the crypto-assets skyrocketed. Nevertheless, given the lack of stable criteria and data on the extremely large fluctuations in the value of crypto-assets, their conversion into conventional currencies should take place immediately after confiscation. Otherwise, the establishment of a specialized team for managing the seized crypto-assets, either at the national or European level, is deemed necessary. The role of this team would be to identify the optimal point in time for liquidating the crypto-assets to maximize the benefit to the state budget.[49]

The EU should intervene with an effective, unified regulatory framework for the confiscation of cryptocurrencies as proceeds of criminal activities, applicable across all Member States. Taking action at European level and integrating a consistent level of regulation for virtual currencies presents clear advantages. It ensures the identification and assessment of risks for participants in this market across the entire EU. The nature of crypto-assets allows their creation in one Member State and use worldwide. Differing levels of regulation by Member States lead crypto-assets businesses and users to choose the most convenient regulation, which can vary depending on the chosen country.[50]

The increased risks associated with the use of crypto-assets and the need to maintain economic stability require a direct regulatory response. Such a response can be even more effective if coordinated internationally. A heterogeneous mix of national regulations does not adequately address emerging risks and concerns of economic stability. Moreover, participants in the market operate on an international scale. Economic stability is undermined by the increased use of crypto-assets, but it can be assisted through systematic control. Transparency regarding amounts, structure, and purpose of crypto-assets is crucial. For this reason, the Euro zone monitors the amounts transferred and exchanged, as well as transaction prices, as it is connected to the 'traditional' financial sector.[51] These challenges mentioned above undermine countries' ability to enforce effective and persuasive sanctions. Each country must address the challenges within its own framework to identify gaps and take appropriate measures. Licensing and registration of crypto-assets exchanges, customer identification/verification requirements, and record-keeping obligations can facilitate countries in enforcing better and more effective measures. For more effective confiscation of crypto-assets as products of crime, countries need to provide sufficient and effective international cooperation. The goal is to assist in combating money laundering and related predicate offenses. Therefore, mutual discovery, enforcement, seizure, and forfeiture of assets and means of crime in the form of crypto-assets need to be facilitated. Adequate

[49] Usman W Chohan, 'Fiscal Experiences with Bitcoin: Bulgarian Case Study' (2018) Discussion, Paper Series: Notes on the 21st Century, 2.
[50] European Banking Authority, 'Opinion on "Virtual Currencies"' (n 31) 46.
[51] European Central Bank, 'Draghi M. Letter (QZ- 045) to Members of the European Parliament' (2017) ECB Public, Frankfurt, L/MD/17/284.

supervision and regulatory control of convertible crypto-assets operating within each country's jurisdiction would enable countries to provide assistance in investigations. The lack of effective regulation and the ability to conduct investigations in most countries hinder substantial international cooperation. Furthermore, many countries lack a legal framework, which allows the criminalization of certain money laundering and terrorism financing activities using crypto-assets, making it difficult to act effectively in cases of dual criminality.[52]

The complete decentralization of crypto-assets is their greatest adversary, with the potential to lead to their demise or make them experimental projects with limited practical use in the broader economy. Establishing a strong payment system requires the existence of a central authority that provides licensing and assumes responsibility for facilitating payments. This authority, among other things, is responsible for facilitating payments and dealing with any issues arising from the activities it supervises. Therefore, the assistance of such an authority would also facilitate the confiscation of crypto-assets as criminal proceeds. However, the idea of a central authority has faced criticism because it creates a private monopoly without fully addressing the problem of responsibility, which is deeply rooted in decentralized cryptocurrencies.[53]

6 THE 5TH DIRECTIVE 2018/843/EU & THE 6TH DIRECTIVE 2018/1673 ON COMBATING MONEY LAUNDERING CONCERNING CRYPTOCURRENCIES, MICA REGULATION & FATF GUIDANCE

In order to address the challenges posed by crypto-assets, the European legislator included in the scope of the legislative framework, as obligated entities, the 'providers of services for the custody of digital wallets'[54] and the 'providers engaged in the exchange services between virtual currencies and fiat currencies'.[55] Member States undertook the obligation to transpose this directive into their national law by 10 January 2020.[56] As obligated entities, providers of services for the custody of digital wallets and providers engaged in exchange services between virtual assets and fiat currencies are required to comply with the requirements imposed on banks and other financial institutions.[57] They must register with the authorities responsible for combating money laundering, implement due diligence controls, monitor crypto-assets transactions, and report any suspicious activity to government authorities.[58]

---

[52] FATF, 'Guidance for a Risk-based Approach to Virtual Currencies' (2015) (n 29) 38.
[53] Asress Adimi Gikay, 'Regulating Decentralized Cryptocurrencies Under Payment Services Law: Lessons from European Union' (2018) 9(1) Law Journal of Law, Technology & the Internet 1, 14.
[54] The definition of 'custodian wallet provider' is attributed to Article 3, paragraph 19 of the 4th Directive on combating money laundering, as amended by Article 1 of the 5th Directive.
[55] Directive 2018/843 (n 26).
[56] ibid Article 4.
[57] European Supervisory Authority, 'Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector' (2019) 17, <https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/1605240c-57b0-49e1-bccf-60916e28b633/Joint%20Opinion%20on%20the%20risks%20on%20ML%20and%20TF%20affecting%20the%20EU%27s%20financial%20sector.pdf?retry=1> accessed 10 December 2023.
[58] Commission, 'Commission Staff Working Document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering

However, after the adoption of the 5th Directive on combating money laundering from criminal activities, there have been changes in the field of crypto-assets. New crypto-assets were created, new types of such services emerged, and new service providers entered this market.[59] In response to these new developments, FATF changed its recommendations in October 2018, which are applicable to financial services involving crypto-assets and similar service providers.[60] In June 2019, FATF issued an interpretative note to Recommendation 15 (INR 15) to further clarify how the requirements should be applied concerning virtual assets and virtual asset service providers. At the same time, new Directives were adopted[61] on applying a risk-based approach to virtual assets and virtual asset service providers. These new Directives focus on points where virtual assets activities intersect with and provide gateways to and from the traditional financial system,[62] such as so-called crypto exchanges. The aim of these new directives is to assist in better understanding the evolution of regulatory and supervisory responses to virtual asset activities by national authorities. Providers of virtual asset services and individuals seeking to engage in digital currency activities should be aware of their obligations related to combating money laundering and should comply effectively.[63]

In the revised form of Recommendation 15, countries are required to control virtual asset service providers for the purposes of combating the laundering of proceeds from criminal activities, license them, and register them.[64] This means that everyone must be subject to an effective system of control and compliance with the measures outlined in the FATF recommendations.[65] Such control provides a balanced and proportional approach, ensuring technical advantages and a high degree of transparency in the field of alternative economies and social entrepreneurship (as per the legislative resolution of the European Parliament on April 19, 2018).[66]

However, a careful examination of recent FATF standards regarding virtual assets in relation to the framework established by the 5th Directive on combating money laundering reveals that the existing regime still deviates from what is currently considered the international 'standard' for combating money laundering from criminal activities and the financing of terrorism concerning crypto-assets. The initial observation is that the definition of 'virtual currencies' in the 5th Directive on Combating Money Laundering from Criminal

and terrorist financing affecting the internal market and relating to cross-border activities' SWD (2019) 650 final, 234.

[59] Houben and Snyers (n 5) 2.

[60] FATF, 'FATF Report to G20 Leaders' Summit' (2019) 6, <https://www.fatf-gafi.org/media/fatf/content/images/G20-June-2019.pdf> accessed 10 December 2023.

[61] FATF, 'Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' (2021) 17 <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf> accessed 10 December 2023.

[62] FATF, 'Guidance for a Risk-based Approach to Virtual Currencies' (2015) (n 29) 46.

[63] FATF, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' (2019) 6 <https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 10 December 2023.

[64] FATF, 'FATF Report to G20 Leaders' Summit' (n 60) 7.

[65] Legal entities should be licensed or registered in the jurisdiction of their establishment or formation, while natural persons should be licensed or registered in the jurisdiction where their business is headquartered. See FATF, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' (2019) (n 63) 22.

[66] FATF, 'FATF Report to G20 Leaders' Summit' (n 60) 7. Commission, 'Commission SWD accompanying Report on the assessment of the risk of money laundering' (n 58) 103.

Activities is narrower than the corresponding FATF definition. It only covers so-called 'cryptocurrencies' and does not encompass other types of virtual assets. This implies that only cryptocurrencies, and no other virtual assets, can be subject to confiscation as proceeds from criminal activities and money laundering.

The second observation[67] is that many participants in the crypto-assets market do not fall within the regulatory scope of the 5th Directive on combating money laundering from criminal activities. Several activities of virtual assets service providers, as defined by the FATF, remain unregulated under the 5th Directive, leaving blind spots in the fight against money laundering and terrorism financing. Specifically, the activities covered by FATF recommendations but not by the 5th Directive on combating money laundering include:[68]

a) Platforms that provide only cryptocurrency-to-cryptocurrency exchange services (i.e., virtual to virtual assets);
b) Platforms that facilitate the transfer of crypto-assets as intermediaries;
c) Individuals actively involved in offering and selling crypto-assets issued by an issuer.

When the 5th Directive on combating money laundering was conceived, it appears that the European legislator did not pay attention to the existence of these factors and the potential risks they might pose.

Furthermore, vigilance regarding these risks has intensified, both among regulatory authorities and at the national level by Member States[69]. To align the European framework for combating money laundering with the modern reality of crypto-assets, the EU should consider a series of regulatory actions. Given the FATF's definition of virtual assets, one initial regulatory action to be considered is expanding the scope of the definition of virtual currencies. This would allow for the confiscation of a broader range of crypto-assets, addressing gaps and vulnerabilities that criminal organizations could exploit to retain their illicit proceeds. Determining how to apply the existing legislative framework when a crypto-asset falls within the regulatory perimeter is not always straightforward.[70]

In June 2019, FATF adopted an Interpretive Note for Recommendation 15 (INR.15) to elucidate the application of FATF requirements concerning virtual assets and virtual assets service providers. Subsequently, FATF conducted two assessments to evaluate the implementation of the revised FATF standards for virtual assets by jurisdictions and the private sector. These assessments revealed progress on the part of both the public and private sectors, yet underscored the need for substantial efforts to achieve global implementation. Following the second 12-month review in June 2021, FATF committed to prioritizing the implementation of FATF Standards on Virtual Assets. In line with this commitment, FATF released an Updated Guidance for a risk-based approach to virtual assets and virtual assets

[67] Houben and Snyers (n 5) 76-80; Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law [2018] OJ L284/22 (Directive 2018/1673), preamble recital 6.
[68] Commission, 'Commission SWD accompanying Report on the assessment of the risk of money laundering' (n 58) 103.
[69] ibid.
[70] European Securities and Markets Authority, 'Advice on Initial Coins Offerings and Crypto-Assets' (2019) 37 <https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf> accessed 10 December 2023.

service providers in October 2021, aiming to provide clarifications for the assistance of jurisdictions in effectively implementing FATF's R.15/INR.15 requirements.[71]

To ensure the ongoing relevance of current anti-money laundering and counter-terrorist financing (AML/CFT) Standards, FATF monitors the developments in DeFi, with a specific focus on the emergence of genuinely decentralized DeFi entities. The aim is to facilitate dialogue on shared challenges in AML/CFT implementation, risk assessment, and the adoption of good practices. Simultaneously, FATF is addressing the persistent and escalating threat of criminal exploitation of Virtual Assets in the receipt and laundering of illicit proceeds from ransomware attacks. Ransomware cybercriminals are increasingly resorting to mixers, tumblers, and privacy coins for receiving and laundering illicit proceeds, with industry insights suggesting that Bitcoin remains the most commonly used virtual asset for such purposes. To counter these threats, recent consultations involving both jurisdictions and the industry have recognized the potential of blockchain analytics in tracing money laundering related to ransomware.[72]

In June 2022, FATF released a targeted update on the implementation of its Standards regarding virtual assets and virtual asset service providers, with a specific focus on the FATF's Travel Rule. This report follows the extension of FATF's anti-money laundering and counter-terrorist financing measures to virtual assets three years ago, aimed at preventing criminal and terrorist misuse of the sector. Addressing the evolving threats of money laundering and terrorist financing, the report underscores the ongoing necessity for FATF to monitor the expansion of DeFi and NFTs markets, as well as the risks associated with unhosted wallets.

In response to the report's findings, FATF strongly urges all countries to expeditiously implement the FATF's Standards on virtual assets and virtual assets service providers. To bolster these implementation efforts, FATF has outlined a series of initiatives. Firstly, FATF is actively promoting the adoption of FATF's R.15/INR.15, which includes the Travel Rule. This initiative involves facilitating discussions with Member States to address common challenges and issues related to implementation. Additionally, FATF is actively raising

---

[71] The 2021 Guidance incorporates updates that specifically address six pivotal areas: 1. Clarification of Definitions: The guidance offers clarification on the definitions of virtual assets and Virtual Asset Service Providers (VASPs). 2. Application of FATF Standards to Stablecoins: Specific guidance is provided on how the FATF Standards apply to stablecoins, recognizing the unique characteristics of these assets. 3. Risk Mitigation for Peer-to-Peer Transactions: Additional guidance is outlined concerning the risks associated with peer-to-peer transactions. 3. The document also explores tools available to countries to mitigate money laundering and terrorist financing risks in this context. 4. Updated Guidance on Licensing and Registration: The 2021 Guidance includes updated recommendations on the licensing and registration processes for Virtual Asset Service Providers (VASPs). 5. Implementation of the Travel Rule: Both the public and private sectors receive additional guidance on the effective implementation of the Travel Rule. 6. Principles of Information-Sharing and Cooperation: The guidance emphasizes principles for information-sharing and cooperation among supervisors of Virtual Asset Service Providers (VASPs). This aspect aims to enhance coordination and collaboration in the regulatory landscape. These updates collectively contribute to a more comprehensive and contemporary framework for addressing challenges and risks within the evolving landscape of virtual assets and Virtual Asset Service Providers.

[72] To reduce the profitability of ransomware attacks and to mitigate its risk, it was shared that it would also be useful for FATF to 1) compile, share and publish typologies and red flag indicators of ransomware attacks and 2) strengthen international cooperation between authorities (both LEAs and supervisors) at international level; 3) continue and strengthen outreach to the private sector to inform them of relevant risks; 4) explore ways to take advantage of various sources of information including information on the blockchain and in STRs; and 5) strengthen cooperation between relevant authorities at the domestic level.

awareness by engaging with influential forums, such as G7/G20 and other high-level policy bodies. Moreover, as part of its ongoing commitment, FATF had a comprehensive review of the progress made and the remaining challenges in the implementation of FATF's Standards on virtual assets and virtual assets service providers for June 2023. This thorough assessment was designed to ensure the efficacy of measures taken and to pinpoint areas that may necessitate additional attention or refinement.

In June 2023, the Financial Action Task Force took steps to enhance its AML/CFT measures for virtual assets and virtual asset service providers, aiming to prevent criminal and terrorist misuse of the sector. However, a noteworthy observation reveals that only 30% of assessed jurisdictions mandate the licensing or registration of VASPs and practical implementation of such measures is even scarcer. This situation raises concerns as unlicensed or unregistered virtual assets service providers operating without proper oversight pose money laundering and terrorist financing (ML/TF) risks, complicating law enforcement efforts. Jurisdictions grappling with challenges in licensing or registration processes are urged to enhance supervision and impose sanctions for non-compliance.

Regardless of the regulatory approach adopted, jurisdictions are advised to actively monitor and supervise their virtual assets service providers population, ensuring strict enforcement of AML/CFT obligations. Notably, jurisdictions with established registration or licensing regimes are making commendable progress in supervising and enforcing AML/CFT obligations. The overarching message is that continuous monitoring and supervision of virtual assets service providers, irrespective of the regulatory strategy, are crucial to guarantee compliance with AML/CFT requirements.

Now marking four years since the extension of global AML/CFT standards to virtual assets and virtual asset service providers, some major virtual asset markets have implemented or are in the process of establishing AML/CFT regulations. Nevertheless, a significant concern persists, as 75% of assessed jurisdictions fall short, being either partially or non-compliant with FATF's requirements. This lag in compliance is notably prominent compared to other sectors within the financial industry. Despite this, there are positive signs of collaboration within the private sector, with certain entities working together to enhance Travel Rule compliance tools. While improvements are evident, the industry still faces challenges. The above report represents the fourth targeted review of the implementation of FATF's Standards on virtual assets, providing an updated assessment of emerging risks and market developments in this evolving field.

The EU lags international standards. European regulations for combating money laundering introduced by the 5th Directive for the Prevention of Money Laundering became outdated long before Member States were required to transpose them into their national legal systems, which was on 10 January 2020. If the EU remains inactive, Member States can take action, given their individual participation in the FATF, and amend their national legislations to comply with FATF's most recent recommendations.[73] However, such national action alone is insufficient and might create legal uncertainty across national borders. To avoid imbalances on an international scale, it is preferable to take regulatory action at a higher level.

A few months after the introduction of the 5th Directive, in October 2018, the 6th Directive on the Prevention of the Use of the Financial System for the Purposes of Money

[73] Houben and Snyers (n 5) 2.

Laundering and Terrorist Financing followed. Despite the already identified weaknesses of the 5th Directive and the gaps that were identified, the legislator does not seem to have taken them into account and rather proceeded to minimal regulations regarding crypto-assets. Specifically, in the preamble of the 6th Directive, it is recognized that 'the use of virtual currencies entails new risks and challenges from the perspective of preventing the legalization of income from illegal activities. Member states should ensure the appropriate treatment of these risks'.[74] This is a general statement that does not substantially address the emerging risks and challenges of cryptocurrencies. It can even be argued that it leaves considerable discretion to Member States to regulate as they see fit. However, such an approach may result in fragmented legal frameworks between the national legal systems of Member States.

Regarding crypto-assets, the 6th Directive states that the definition of assets includes assets of any form, including electronic or digital assets, which demonstrate ownership or rights to acquire such assets.[75] In general, the rules introduced by the 6th Directive for combating money laundering do not introduce anything new, and the adoption of a 7th Directive aimed at addressing identified risks and problems within the existing framework would not be surprising. The successive introduction of new legislations for combating the legalization of income from criminal activities in a short period of time strongly indicates the uncertainty in which the European legislator finds itself in. It seems to be struggling to coordinate with the technological developments, as the enacted legislations appear inadequate and outdated even before they are incorporated into the national legal systems.[76]

MONEYVAL had some very useful insights regarding confiscation of virtual assets. More specifically, MONEYVAL members were requested recently to provide information regarding the procedures they apply to implement interim measures for freezing and seizing virtual assets. Seven members submitted relevant information. The majority expressed their intent to seek assistance from virtual asset service providers overseeing suspected criminal proceeds in virtual assets, instructing them to freeze the assets. Some members mentioned using official or government wallets for the transfer and retention of seized virtual assets. The effectiveness of seizing and transferring virtual assets not under the control of a virtual assets service providers, which hold the wallet keys, is dependent on law enforcement agencies obtaining the wallet keys, thereby gaining control of the virtual assets. MONEYVAL members also mentioned utilizing Financial Intelligence Unit (FIU) postponement powers to promptly freeze assets during the pre-trial stage, awaiting the application of more formal means of asset freezing and seizure. Some members indicated attempts to directly engage foreign virtual assets service providers for assistance in seizing and freezing assets, acknowledging the significant dependency on the willingness of VASPs to cooperate voluntarily.[77]

The focal point of recent legislation pertaining to virtual assets is the Markets in Crypto-Assets Regulation. This legislation emerged as the EU's response to the policy

[74] Directive 2018/1673 (n 67) Title 6, Preamble.
[75] ibid Article 2(2).
[76] European Banking Authority, 'Report with advice for the European Commission on crypto-assets' (2019) <https://eba.europa.eu/eba-reports-on-crypto-assets> accessed 10 December 2023; European Securities and Markets Authority (n 70) 20-21.
[77] MONEYVAL Secretariat, Directorate General of Human Rights and Rule of Law, Council of Europe, 'Money Laundering and Terrorist Financing Risks in the world of virtual assets' (2023) Typologies Report, 24 <https://rm.coe.int/moneyval-2023-12-vasp-typologies-report/1680abdec4> accessed 10 December 2023.

discussions triggered by the Libra proposal in June 2019. The debate on whether the crypto-assets market should fall under EU regulation leaned towards an unequivocal affirmative stance. The chosen instrument, a Regulation, clearly underscores the gravity of regulatory intentions. Its objective is to fill a significant regulatory void and establish a harmonized approach to crypto-assets across the EU Single Market.[78]

It is a crucial component of the EU's Digital Finance Strategy and is designed to offer legal certainty for unregulated crypto-assets.[79] The MiCA Regulation, proposed by the Commission, stands as the first comprehensive regulation directly addressing crypto-assets. Its primary objectives are to foster innovation, preserve financial stability, maintain market integrity, and safeguard investors from potential risks. MiCA specifically governs a distinct asset class, crypto-assets, which differs from digital securities, such as stocks and bonds. Formulated in conjunction with existing legislative frameworks, MiCA's scope encompasses the entire crypto-asset ecosystem, leaving no crypto-asset unregulated. The regulation is driven by four main goals:

a) to establish legal certainty with a robust legal framework, clearly defining rules applicable to all crypto-assets not covered by existing financial legislation;
b) to create a legal framework that is both secure and proportionate, fostering innovation and ensuring fair competition;
c) to implement sufficient levels of consumer and investor protection, mitigating the potential risks posed by crypto-assets to the internal market;
d) to ensure financial stability, with a specific mention of stablecoins by the European Commission, recognizing their potential to gain widespread acceptance and pose systemic risks.[80]

7 THE RISK OF ABUSIVE SELECTION OF THE MOST FAVORABLE REGIME (FORUM SHOPPING)

Within the same framework of analysis of the issues regarding cryptocurrencies, there is the risk of abusive selection of the most favorable regime. This arises from the possible divergent incorporation of existing definitions within national laws. Additionally, in the analysis of the European banking authority and the European securities and markets authority, it is mentioned that a significant number of crypto-assets and related activities do not fall under the scope of European financial services legislation.[81] Each Member State is fundamentally free to establish its rules regarding 'unregulated' assets.[82] Some EU Member States have

[78] Dirk Andreas Zetzsche, Filippo Annunziata, Douglas W Arner, and Ross P Buckley, 'The Markets in Crypto-Assets Regulation (MICA) and the EU Digital Finance Strategy' (2020) European Banking Institute Working Paper Series No. 2020/77, University of Luxembourg Law Working Paper Series No. 2020-018, University of Hong Kong Faculty of Law Research Paper No. 2020/059 <https://ssrn.com/abstract=3725395> accessed 10 December 2023.
[79] Tina van der Linden and Tina Shirazi, 'Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets?' (2023) 9 Financial Innovation 22 <https://jfin-swufe.springeropen.com/articles/10.1186/s40854-022-00432-8> accessed 10 December 2023.
[80] van der Linden and Shirazi (n 79) 22.
[81] European Banking Authority, 'Report with advice for the European Commission on crypto-assets' (n **Fel! Bokmärket är inte definierat.**), European Securities and Markets Authority (n 70) 20-21.
[82] Claude Brown, Tim Dolan, and Karen Butler, 'Crypto-Assets and Initial Coin Offerings' in Jelena Madir, *Fintech: Law and Regulation* (Edward Elgar Publishing 2019) 79.

implemented such regulation since late 2018 because 'unregulated' assets pose similar risks to other crypto-assets and those subject to EU legislation on financial services.[83]

These national initiatives are not consistent with each other, leading to divergent approaches within the EU and providing the opportunity for an abusive selection of the most favorable jurisdiction.[84] A crypto-asset regulated by legislation in one jurisdiction may not be regulated in another. This practice can pose a challenge both for combating money laundering and for the overall development of legal schemes for crypto-assets.[85] Cryptocurrency assets constitute an international phenomenon. They are created by private actors in various countries around the world, possess international reach and infrastructure, and are readily accessible, transferable, exchangeable, and tradable from anywhere in the world. As a result, regulatory challenges are not confined to European borders but extend much further. To address these challenges, regulatory authorities' intervention is necessary. In some countries, legislators have already taken action or intend to do so. The problem is that these national initiatives are not aligned with each other, leading to an abusive selection of the most favorable regime. To tackle this issue, regulatory control over cryptocurrency assets should be exercised at European level, preferably in alignment with international standards.

Money laundering and terrorism financing, like cryptocurrency assets, are not limited by European borders.[86] Criminals and terrorists identify gaps and seek 'loopholes' in the regulatory framework to carry out money laundering activities. Therefore, if a country or region has more favorable anti-money laundering rules for cryptocurrency assets compared to the EU, illicit activities are likely to shift to that region, creating gateways for money laundering. The same unquestionably applies to money laundering and terrorism financing activities involving cryptocurrency assets.[87] If consistent anti-money laundering standards were upheld in all regions, the chances of effectively eradicating such activities would be much higher. Hence, it is advisable to establish international standards for combating money laundering through the use of cryptocurrencies. The FATF, as an international policymaking body, aims to achieve precisely this goal. EU Member States should continue to contribute to these efforts, while international standards set by the FATF should continue to be incorporated into European law promptly and coherently, ensuring compliance throughout the internal market and the international financial system.[88]

Instances may arise where virtual assets, deemed proceeds of crime in one country, are located in a foreign jurisdiction. In such scenarios, legal enforcement authorities encounter additional obstacles in freezing or seizing these virtual assets, as they are not under the control of virtual assets service providers established within the jurisdiction. This highlights

---

[83] Steven Maijoor, 'Crypto-Assets: time to deliver in Keynote speech 3rd Annual FinTech Conference' (2019) 6 <https://www.esma.europa.eu/sites/default/files/library/esma71-99-1120_maijoor_keynote_on_crypto-assets_-_time_to_deliver.pdf> accessed 10 December 2023.

[84] European Banking Authority, 'Report with advice for the European Commission on crypto-assets' (n **Fel! Bokmärket är inte definierat.**) 15.

[85] Brown, Dolan, and Butler (n 82) 79.

[86] Council of the European Union, 'Council Conclusions on strategic priorities on anti-money laundering and countering the financing of terrorism' (2019) 14823/19, 4 <http://data.consilium.europa.eu/doc/document/ST-14823-2019-INIT/en/pdf> accessed 10 December 2023.

[87] Brown, Dolan, and Butler (n 82) 79.

[88] Houben and Snyers (n 5) 2.

the crucial role of effective international cooperation in pursuing such cases and executing asset freezes or seizures. Jurisdictions offering practical insights on handling such situations frequently cited the use of international cooperation channels, such as Mutual Legal Assistance (MLA). Respondents expressed skepticism about the efficiency of these mechanisms in ensuring the timely seizure or freezing of virtual assets.[89]

8 CONCLUSIONS

In conclusion, four years after enhancing its standards to address virtual assets and virtual asset service providers, the global implementation of these measures remains notably ineffective. Nearly three-quarters of jurisdictions exhibit only partial or no compliance with FATF requirements, with many jurisdictions yet to implement fundamental measures. A significant concern arises from the fact that over half of the survey respondents have not initiated the implementation of the Travel Rule, a crucial FATF requirement aimed at preventing the transfer of funds to sanctioned individuals or entities. This lack of regulation creates substantial loopholes for criminal exploitation, emphasizing the urgent need to address gaps in the global regulation of virtual assets.

Recognizing the severity of the situation, the FATF has called upon all countries to promptly apply Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) rules to virtual asset service providers, without further delay. In a report published on 27 June, the FATF urged countries to expeditiously implement its Recommendations on virtual assets and virtual assets providers, including the Travel Rule, to close these regulatory loopholes. Looking ahead, in the first half of 2024, the FATF plans to publish a table illustrating the steps taken by FATF member jurisdictions and other jurisdictions with materially important virtual assets service providers activities toward implementing Recommendation 15. This underscores the ongoing commitment to monitor and enhance the regulatory landscape surrounding virtual assets on a global scale.

The FATF has consistently updated its standards on asset recovery as part of its overarching commitment to bolster countries' efforts in depriving criminals of their unlawfully obtained gains. In pursuit of this objective, the FATF is set to introduce new mechanisms that countries should adopt to efficiently freeze, seize, and confiscate criminal assets, both at the domestic level and through international collaboration. The Plenary has reached a consensus to commence work on revising Recommendations 4 (non-conviction based confiscation) and 38 (prompt action in response to requests by countries to identify, freeze, and seize property). The intended approval of these revisions is slated for October 2023, reflecting the FATF's ongoing dedication to enhancing global measures for combating financial crime and promoting asset recovery.[90]

Blockchain tools have played a crucial role in supporting successful enforcement cases, implementing targeted financial sanctions, and taking other actions to disrupt ransomware financing. However, industry stakeholders acknowledge persistent challenges, particularly arising from the use of privacy coins, chain-hopping via non-compliant virtual asset service providers, and unhosted wallets. To effectively address these challenges in moving forward,

[89] MONEYVAL, 'Money Laundering and Terrorist Financing Risks in the world of virtual assets' (n 77) 36.
[90] Bruce Zagaris, 'Money Laundering, Bank Secrecy, and International Human Rights' (2023) 39(7) International Enforcement Law Reporter 240.

it is imperative for both jurisdictions and the private sector to implement FATF's Standards on virtual assets and virtual asset service providers. This implementation is crucial for enabling the private sector to identify illicit actors and detect suspicious transactions.

While the MiCA Regulation represents an ambitious legislative initiative as referred to above, there are notable areas that require refinement. There is an absence of a systematic approach to EU law, with a need for the incorporation of thresholds and concepts from other EU law sources into MiCA. There is also a notable gap in providing a framework for supervisory cooperation concerning truly global stablecoins. On a broader scale, MiCA is part of a comprehensive approach deemed essential, yet substantial revisions are necessary to achieve its varied goals. MiCA aims to establish legal certainty by creating a uniform framework directly applicable in Member States. Institutions, such as the ECB have welcomed regulation for crypto-assets, and MiCA applies to anyone offering crypto-assets or providing crypto-asset services in the EU. The regulation, in Article 2, specifies that it applies to currently unregulated crypto-assets outside the scope of existing financial services legislation, ensuring continuity for those covered by MiFID II/MiFIR. Despite the current challenges, there is hope that, with amendments, the MiCA Regulation will eventually contribute to a regulated environment for crypto-assets, allowing European citizens and businesses to safely benefit from their advantages, aligning with the Commission's Digital Finance Package objectives.

LIST OF REFERENCES

Adimi Gikay A, 'Regulating Decentralized Cryptocurrencies Under Payment Services Law: Lessons from European Union' (2018) 9(1) Law Journal of Law, Technology & the Internet 1

Brown C, Dolan T, and Butler K, 'Crypto-Assets and Initial Coin Offerings' in Madir J, *Fintech: Law and Regulation* (Edward Elgar Publishing 2019)
DOI: https://doi.org/10.4337/9781788979023.00016

Chohan UW, 'Fiscal Experiences with Bitcoin: Bulgarian Case Study' (2018) Discussion, Paper Series: Notes on the 21st Century

Crotty J, 'Structural causes of the global financial crisis: A critical assessment of the new "financial architecture"' (2009) 33(4) Cambridge Journal of Economics 563
DOI: https://doi.org/10.4337/9781784719029.00013

Czarnecki J, 'Digital Currencies and the Anti-money Laundering/Counter- terrorism Financing Regulations in the EU: Imaginary Risk or Real Challenge?' in Ligeti K and Simonato M (eds), *Chasing Criminal Money, Challenges and perspectives on asset recovery in the EU* (Hart Publishing 2017)
DOI: https://doi.org/10.5040/9781509912087.ch-013

Haynes A and Yeoh P, *Cryptocurrencies and Cryptoassets: Regulatory and Legal Issues* (Routledge 2020)
DOI: https://doi.org/10.4324/9781003034599

Heine S, 'Bitcoins und Botnetze – Strafbarkeit und Vermögensabschöpfung bei illegalem Bitcoin-Mining' (2016) NStZ 441

Hilgendorf E et al, *Informationsstrafrecht Und Rechtsinformatik* (Logos Berlin 2004)

Houben R and Snyers A, 'Crypto-assets: Key Developments, Regulatory Concerns and Responses' (2020) Study Requested by ECON committee <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf> accessed 10 December 2023

Mylonopoulos C, *Criminal Law, General Part* (P.N. Sakkoulas 2008)

Mylonopoulos C, 'Is issuance possible in the USA for legitimizing cryptocurrencies derived from criminal activity' (2018) Criminal Chronicles 185

Papadimitrakis G, 'Legitimization of Income from Criminal Organization and Cryptocurrencies' (2018) 9 Armenopoulos 1598

Spoenle J, 'Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?' (2010) Discussion Paper prepared for the Economic Crime Division of the Council of Europe <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3df> accessed 10 December 2023

Stamati, *Systemic Interpretation of Criminal Law* (P.N. Sakkoulas 2005)

Teichmann FMJ and Falker MC, *Cryptocurrencies and financial crime: solutions from Lichtenstein* (2021) 24(4) Journal of Money Laundering Control 775
DOI: https://doi.org/10.1108/jmlc-05-2020-0060

Thomas Fischer, *Strafgesefzbuch* (64th edn, C.H. Beck 2017)

van der Linden T and Shirazi T, 'Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets?' (2023) 9 Financial Innovation <https://jfin-swufe.springeropen.com/articles/10.1186/s40854-022-00432-8> accessed 10 December 2023
DOI: https://doi.org/10.1186/s40854-022-00432-8

Vigna P and Casey MJ, *Cryptocurrency- how bitcoin and Digital Money are Challenging the Global Economic Order* (St. Martin's Publishing Group 2015)

Wabnitz HB and Janovsky T, *Handbuch des Wirtschafts und Steuerstrafrechts* (4th edn, C.H. Beck 2014)

Wolff H et al, *Strafgesetzbuch. Leipziger Kommentar* (12th edn, De Gruyter 2008)

Zagaris B, 'Money Laundering, Bank Secrecy, and International Human Rights' (2023) 39(7) International Enforcement Law Reporter 240

Zetzsche DA, Annunziata F, Arner DW, and Buckley RP, 'The Markets in Crypto-Assets Regulation (MICA) and the EU Digital Finance Strategy' (2020) European Banking Institute Working Paper Series No. 2020/77, University of Luxembourg Law Working Paper Series No. 2020-018, University of Hong Kong Faculty of Law Research Paper No. 2020/059 <https://ssrn.com/abstract=3725395> accessed 10 December 2023
DOI: https://doi.org/10.2139/ssrn.3725395