Northumbria University
NEWCASTLE

Law School

Northumbria Legal Studies Working Paper Series

Digital currencies: an analysis of its present regulation in the UK: A collaborative essay by NINSO, the Northumbria Internet & Society Research Interest Group

Rachel Allsopp, Dr Guido Noto La Diega, Samantha Rasiah, Ann Thanaraj, and Daria Onitiu

Northumbria Legal Studies Working Paper No. 2019/03

University of Northumbria at Newcastle – School of Law

DIGITAL CURRENCIES: AN ANALYSIS OF ITS PRESENT REGULATION IN THE UK': A COLLABORATIVE ESSAY BY NINSO, THE NORTHUMBRIA INTERNET & SOCIETY RESEARCH INTEREST GROUP

Dr Guido Noto La Diega, Rachel Allsopp, Samantha Rasiah, Ann Thanaraj, and Daria Onitiu

Digital currencies, whilst being an innovative payment method, poses several regulatory challenges in light of the possibilities to be used for a criminal purpose. This collaborative essay illustrates a brief report, which intends to provide for a general outlook on the UK's effort in understanding the risks digital currencies pose to financial crime, money laundering, terrorist financing and cybercrime. This premise paves the way for ensuring the balance between protection of essential interests and innovation, most notably, in ensuring the implementation of the 5th Money Laundering Directive.

The present contribution is prepared by the Northumbria Internet & Society Research Interest Group (NINSO). The NINSO group is multidisciplinary research group that shares research interests on technology and its significance in law, computer-science, social sciences, and engineering. Being interested in a holistic outlook of technological developments, it frequently organises seminars that aim to strengthen both, collaborations and the quality of academic research in this area.

Keywords: digital currencies, security, United Kingdom

Understanding the risks of digital currencies:

The UK Government and associated bodies have applied considerable effort in understanding the risks of virtual currencies with regard to financial crime, money laundering, terrorist financing and cybercrime. This finding is supported by the reports of the HM Treasury, The UK National Crime Agency and the National Cyber Security Centre.

The HM Treasury conducted intelligence gathering with regard to the use of digital currencies and cybercrime. The HM Treasury Office's report in 2017 outlined three possible ways the use of virtual currencies enhances cybercrime.[1] The first consideration is that virtual currencies directly enable victim payments to cyber criminals. Secondly, virtual currencies constitute an important way of payment of illicit goods and services. Finally, "virtual currencies play a significant role in laundering the proceeds of cyber dependent crime."[2]

With regard to the threat of cybercrime posed by digital currencies, a recent report published by the UK National Crime Agency (NCA) focused on encrypted services, such as the dark web. The 2018 report states "the use of technologies such as the dark web, encryption, virtual private networks (VPN) and virtual currencies will support fast, 'secure' and anonymous operating environments, facilitating all levels of criminality."[3] The findings of the NCA outline that the sale of drugs dominates the illicit trade on the dark web, albeit there are "niche sites" where commodities, such as firearms and CSEA materials are for sale.[4] Modern dark net markets build on the exchange of crypto currencies, such as Bitcoin and other modified crypto currencies, such as Ripple and Ethereum, supporting a trend of illegal trading that is likely to continue in the future.[5]

The extent to which cybercrime affects business has been considered by The National Cyber Security Centre (NSCS) in its 2017-2018 report[6]. The report identifies that there has been an increase in the use of cryptocurrency mining without the consent of an individual's computer throughout 2017. Known as "cryptojacking" cyber criminals use a visiting computer's spare computer processing power to mine

---

[1] HM Treasury and Home Office, 'National risk assessment of money laundering and terrorist financing 2017' (October 2017) < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf> accessed 5 October 2018 at page 40.
[2] ibid.
[3] National Crime Agency, 'National Strategic Assessment of Serious and Organised Crime' (2018) < http://www.nationalcrimeagency.gov.uk/publications/905-national-strategic-assessment-for-soc-2018/file> accessed 5 October 2018 at [54].
[4] ibid [76]- [77].
[5] ibid [75], [78].
[6] 'The Cyber Threat to UK Business', National Cyber Securiy Centre (NCSC) and National Crime Agency (NCA) Report, 2017-2018 <https://www.ncsc.gov.uk/cyberthreat>

the virtual currency "Moreno". Further, the report argues that the anonymity ensured by virtual currencies enables cyber criminals to conduct ransomware attacks and make profit. For this premise, the report refers to the WannaCry ransomware attacks and to ransom Distributed Denial of Service attacks. The NSCS acknowledged that following the WannaCry attack, hackers might be encouraged to use the faster method of spreading malware through networks. While the NCSC and the NCA focus on an increased cooperation with law enforcement and an improvement of the NHS networks, both are still working on avenues to mitigate global attacks when using ransomware.

It should be borne in mind, when considering strengthening of regulatory measures on the basis of concerns about money laundering, that there is as yet insufficient evidence to suggest that virtual currencies are more likely to be used for money laundering than cash. Privacy and anonymity are central to what could make virtual currencies appealing for money laundering. However, even with the more private coins, such as Monero, there are recent analyses which have demonstrated that there are ways to trace transactions and find "privacy-sensitive" data.[7] Once identities have been revealed by law enforcement agencies, the crypto-money launderer is in a worse position than the cash money launderer. The immutability of transaction data, means that there is substantial evidence available to law enforcement agencies to use in prosecutions. In contrast, it is possible for cash transactions undertaken in the process of money laundering to be entirely unrecorded.

Based on these considerations, the UK should adopt a clear regulatory framework in accordance with the risks identified, i.e. money laundering, tax invasion and financing of terrorism. In this respect, the UK has taken effective steps with regard to the compliance of the MLR 2017 Regulation and has found better ways in finding avenues to freeze crypto assets. The HM Revenue & Customs established that certain transactions can be taxed, depending on the circumstances. A further development is the regulatory framework that helps banks to mitigate financial crimes caused with the aid of cryptocurrencies. Based on these considerations, the UK should continue to closely cooperate with the Financial Action Task Force (FAFT), implementing their recommendations. Finally, the implementation of the 5th Money Laundering Directive is vital to establish a level of regulatory oversight over the use of digital currencies.[8]

In this respect, the UK has taken effective steps with regard to the compliance with Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017

[7] Möser, Soska et al (2018) The authors of the report go on to suggest countermeasures to increase the privacy of Monero; Aldridge and Askew (2017) highlight a kind of arms race between law enforcement agencies and criminals using blockchain technology (focusing on cryptomarkets).
[8] House of Commons and Treasury Committee, Crypto-assets (Twenty-Second Report of Session 2017–19, 19 September 2018) at [105].

Regulations) regulations 33 (1) (b) and s. (33) (6) (c). HM Treasury Office in an advisory note supplied the requirement of enhanced customer due diligence measures and monitoring in any business relationship with a high-risk third country, as regulated by s. 33 (1) (b) of the MLR 2017 Regulations.[9] In addition, it intends to take account of new jurisdictions that are of high-risk deficiencies in their anti-money laundering and counter-terrorism regimes in light of MLR 2017 Regulation 33(6)(c) and the findings of the FATF.[10] Current efforts by the HM Treasury Office build on published statements by the FATF that there are jurisdictions with major flaws in their anti- money laundering and countering the financing of terrorism regimes.[11] Reference is made to the FATF's statements to apply counter-measures against the Democratic People's Republic of Korea and to apply enhanced due diligence measures against Iran, which should be proportionate to the risks arising from the jurisdiction.[12]

The UK has made considerable effort to better locate a regulated exchange or the asset owner in terms of freezing those assets. In the *R v Teresko* case, the Crown Court (Kingston upon Thames) held that cryptocurrencies or their proceeds of sale could be subject to a restraint order or confiscation order to the extent that they constitute "realisable property", falling under s. 47 of the Proceeds of Crime Act 2002.[13] However, problems in freezing digital currencies persist, due to their appearance in encrypted software wallets and the fact that those assets are not held by a third party.[14] Because virtual currencies are anonymously held and are part of a decentralised distributed ledger without a regulated custodian, it may be difficult to discover and freeze the defendant's cryptocurrency assets.

Implementing the Fifth Anti-Money Laundering Directive (5AMLD) into UK's national law will help to better locate a regulated exchange or the asset owner and freeze those assets. One effective method to freeze the assets is through the digital asset exchange platforms. While virtual currencies are based

---

[9] 'HM Treasury Advisory Notice: Money Laundering and Terrorist Financing control in higher risk jurisdiction' (11 July 2018) < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/724843/Money_laundering_and_terrorist_financing_controls_in_overseas_jurisdictions___advisory_notice.pdf> accessed 5 October 2018 at page 1.

[10] ibid.

[11] FAFT, 'Outcomes FATF-MENAFATF Joint Plenary' (27-29 June 2018) < http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-june-2018.html#TEN> accessed 5 October 2018.

[12] 'HM Treasury Advisory Notice: Money Laundering and Terrorist Financing control in higher risk jurisdiction' (11 July 2018) < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/724843/Money_laundering_and_terrorist_financing_controls_in_overseas_jurisdictions___advisory_notice.pdf> accessed 5 October 2018 at pages 4-5.

[13] *R v Teresko (Sergejs)* [2018] Crim. L.R. 81; Jonathan Hall, 'Case Comment Restraint orders: R. v Teresko (Sergejs)' [2018] 1Crim. L.R 81, 82-84.

[14] Michael Bahar, Greg Kaufman and Kristen Bertch, 'Insight: Enforcing the Crypto Freeze' (Bloomberg Law, 28 September 2018) < https://www.bna.com/insight-enforcing-crypto-n73014482903/> accessed 5 October 2018.

on various security measures, such as cryptographic protocols, and thus do not show any personal information of the user, the blockchain technology requires that the transactions are shown on a public register. As a result, if you know the relevant exchange, which mostly contains private keys for customers or "know-your-customer" records that connect defendants to their account, it is possible to enforce the freeze without the defendant's prior knowledge. This is because digital currencies transactions can be tracked with the relevant IP addresses.

It is important to note, however, that this hurdle can be circumvented by further technologies, such as *Tor* or *IpBouncing*, which further supports the anonymity of the users. A further method that enhances the anonymity of users is the use of "mixers". Christina Carata describes that "mixing wallets" are "services accepting crypto coins and returning the same amount, minus a services charges, in the same virtual currency but the new coins are not associated by the original ones." While these risks need to be kept in mind, the 5AMLD will ensure progress in collecting the information necessary to identify the parties involved in any of their transactions. This new anti-money laundering regulation requires exchanges to both report suspicious transaction activity and run identification and verification checks on their customers.

The UK is further finding possibilities to impose a tax on certain cryptocurrencies. As to the definition of cryptocurrencies, such as Bitcoin, the UK treats them as private money for tax purposes, because no VAT is charged when executing Bitcoin for pound sterling. Nevertheless, the policy brief published by HM Revenue & Customs in 2014 outlines how certain cryptocurrency transactions can be taxed depending on the circumstances.[15] Instances where the VAT is exempt include when the income is received from Bitcoin mining activities, the income is received by miners for other activities relating to the verification of transactions entailing specific charges as well as any charges made over and above the value of the Bitcoin for the arrangement of transactions in Bitcoin.[16] VAT will be charged from suppliers of any goods and services in exchange for any cryptocurrency.[17]

John Barrdear and Michael Kumhof, in their recent article, studied the consequences of issuing a central bank digital currency which would effectively treat digital currencies as property for taxation purposes.[18] According to their working paper, the central bank could "maintain all of the copies of the

[15] HM Revenue and Customs, 'Policy paper: revenue and Customs Brief 9 (2014): Bitcoin and other cryptocurrencies' (3 March 2014) < https://www.gov.uk/government/publications/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies> accessed 5 October 2018.
[16] ibid.
[17] ibid.
[18] John Barrdear and Michael Kumhof, 'The macroeconomics of central bank issued digital currencies' (Working Paper No 605, 18 July 2016) < https://www.bankofengland.co.uk/working-paper/2016/the-macroeconomics-of-central-bank-issued-digital-currencies> accessed 5 October 2018; Octavian Nica, Karolina Piotrowska, Klaus Reiner Schenk-Hoppe,

ledger itself, public institutions could maintain copies for each other, or private sector agents could be involved in collaboration with the central bank."[19] In this respect, the Bank of England established a research unit that currently investigates the introduction of a cryptocurrency linked to pound sterling.[20]

The UK is in the process of detecting measures that banks can take to handle financial crimes caused with the aid of cryptocurrencies. The UK Financial Conduct Authority, in a letter addressed to the CEO, expressed their opinion on measures banks should take with regard to cryptocurrencies in order to handle their financial crime risks.[21] It recommends an enhanced scrutiny of clients and their activities where bank services entail a crypto-asset exchange, where there is a conversion of a cryptocurrency and a fiat currency or where the bank maintains a trading relationship with a client whose wealth derives from crypto-assets.[22] In these circumstances, the bank's financial crime framework should be equipped against the risks posed by activities related to cryptocurrencies, which entails the communication with clients about the risks and the employment of due diligence procedures.[23]

Even though the FCA does not regulate cryptocurrencies, since they are not considered to be commodities or currencies under the Markets in Financial Instruments Directive II (MIFID II), a FCA statement on the 6th April 2018 indicates that derivatives which use cryptocurrencies as the underlying investment are regulated. The statement underlines that cryptocurrency derivatives are classified as financial instruments under the MIFID II and therefore, firms involved in activities involving cryptocurrency derivatives must comply with all applicable rules in the FCA's handbook and any directly applicable EU regulation.[24]

On an international level, key recommendations help to provide a better understanding of the risks associated with cryptocurrencies, assisting in the mitigation of risks with the aid of rules of universal

---

'Cryptocurrencies: Economic benefits and risks' (University of Manchester FinTech working paper no 2, 26 October 2017) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3059856> accessed 5 October 2018 at page 32.

[19] John Barrdear and Michael Kumhof, 'The macroeconomics of central bank issued digital currencies' (Working Paper No 605, 18 July 2016) < https://www.bankofengland.co.uk/working-paper/2016/the-macroeconomics-of-central-bank-issued-digital-currencies> accessed 5 October 2018 at pages 7-8.

[20] Robert Mendick, 'Bank of England plots its own bitcoin-style digital currency' (*The Telegraph*, 30 December 2017) < https://www.telegraph.co.uk/news/2017/12/30/bank-england-plots-bitcoin-style-digital-currency/> accessed 5 October 2018; further information can be found here: House of Commons and Treasury Committee, Crypto-assets (Twenty-Second Report of Session 2017–19, 19 September 2018) at [38]- [40].

[21] Shearman & Sterling LLP, 'UK Regulator Sets Out Good Practice For Handling Financial Crime Risks From Crypto-Assets' (*Mondaq Business Briefing*, 26 June 2018) < http://www.mondaq.com/uk/x/712870/White+Collar+Crime+Fraud/UK+Regulator+Sets+Out+Good+Practice+For+Handling+Financial+Crime+Risks+From+CryptoAssets> accessed 6 October 2018.

[22] ibid.

[23] ibid.

[24] Financial Conduct Authority, 'Cryptocurrency derivatives' (6 April 2018) < https://www.fca.org.uk/news/statements/cryptocurrency-derivatives> accessed 8 October 2018.

application. The Financial Action Task Force (FATF) have taken steps with regard to the regulation and enactment of digital currencies. Their framework intends to establish a set of key recommendations with regard to combatting terrorist financing and money laundering.[25] Their rules intend to be of international application, and the aim is to implement the recommended framework, entailing risk assessments, the application of enhanced due diligence measures concerning convertible decentralised digital currencies, internal cooperation, setting up registration/licensing requirements, establishing proportionate criminal, civil and administrative sanctions, the effective international cooperation and preventative measures by financial institutions to combat money laundering.[26] A recent report issued by the FATF in light of the G20 summit in Argentina this year further underlined that it "will continue its work on FinTech and virtual currencies, including considering how to promote and ensure a more coherent and consistent approach by countries to mitigating the risks and supporting financial innovation."[27]

The European Banking Authority (EBA) suggested a that regulatory and supervisory framework be put in place. The EBA delivered an Opinion in 2014 concentrating on the risks of virtual currencies and the risk it poses if not regulated.[28] The Opinion identifies several risks for users, to other market participants, to financial integrity, such as money laundering and other financial crime, risks to payment systems in fiat currencies and risks to regulators.[29] The Opinion recommends "governance requirements for several market participants, the segregation of client accounts, capital requirements and the creation of 'scheme governing authorities' that are accountable for the integrity of a virtual currencies' scheme and its key components, including its protocol and transaction ledger."[30] An immediate response would be the discouragement of credit institutions, payment and e-money institutions from buying and selling virtual currencies. Finally, market participants engaged with virtual currency exchanges shall become "obliged entities" under the EU Anti Money Laundering Directive.

---

[25] FAFT, 'Guidance For A Risk-Based Approach Virtual Currencies' (June 2015) < http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 5 October 2018 at [13]- [14], [23], [28], [29], [33], [38]- [39], [41].
[26] ibid.
[27] FAFT, 'FAFT Report to the G20 Finance Ministers and Central Bank Governors' (March 2018) < http://www.fatf-gafi.org/media/fatf/documents/FATF-G20-FM-CBG-March-2018.pdf> accessed 5 October 2018 at [41]; see also G20 Argentina, 'Communiqué Finance Ministers & Central Bank Governors' (19-20 March 2018, Buenos Aires, Argentina) <https://g20.org/sites/default/files/media/communique_-_fmcbg_march_2018.pdf> accessed 5 October 2018 at [12].
[28] European Banking Authority, 'EBA Opinion on "virtual currencies"' (4 July 2014) < https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> accessed 5 October at [12], [64].
[29] ibid [67].
[30] ibid page 5.

Regulating digital currencies and striking the right balance between safeguarding the business and consumer interests and maintaining innovation:

A close cooperation with the European Blockchain Partnership will effectively fulfil the aim to ensure consumer protection and maintain innovation. Current efforts to strike the balance between innovation and consumer protection are based on the EU FinTech Action Plan, the Cryotoassets Task Force Team and the self-regulatory CryptoUK body. At this stage, it is not clear in what way the use of cryptocurrencies with blockchain technology is compliant with the GDPR. In this respect, the UK's involvement in "the Declaration on the establishment of a European Blockchain Partnership" should offer guidance in how to enhance innovation and respect data protection.

The EU FinTech Action Plan can offer guidance in understanding how to strike the balance between innovation and consumer protection with regard to cryptocurrencies. As stated in the FinTech Action Plan report, the aim is to "to enhance potential financial stability, market integrity, investor and consumer protection, data protection and to mitigate money laundering and terrorist financing-related risks."[31]

The Cryptoassets Task Force team, consisting of staff from the Treasury, the Bank of England and the Financial Conduct Authority will further investigate the benefits and risks of virtual currencies concerning FinTech businesses.[32]

In this respect, a blockchain infrastructure would enable more financial stability and ensure mitigation of money laundering and terrorist financing-related risks. In April 2018, 26 European countries, amongst which was the UK, signed a "Declaration on the establishment of a European Blockchain Partnership."[33] The idea involves the launch of a blockchain infrastructure across the Digital Single Market, acknowledging the benefits to the private and public sector.[34] With reference to an article by Andres Guadamuz and Chris Marsden on cryptocurrencies, because a blockchain application has an

[31] European Commission, 'FinTech Action plan: For a more competitive and innovative European financial sector' (8 March 2018) < https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0109&from=EN> accessed 7 October 2018 at 1.1.
[32] HM Treasury 'Cryptoassets Taskforce meets for the first time' (21 May 2018) <https://www.gov.uk/government/news/cryptoassets-taskforce-meets-for-the-first-time> accessed 8 October 2018; Harry Wilson, 'Crypto assets task force to boost fintech' (*The Times*, 22 March 2018) <https://www.thetimes.co.uk/article/crypto-assets-task-force-to-boost-fintech-ts3g8tnmg> accessed 8 October 2018.
[33] European Commission, 'European countries join Blockchain partnership' (10 April 2018) < file:///C:/Users/w17024841/Downloads/2018DeclarationonEuropeanPartnershiponBlockchainpdf.pdf> accessed 7 October 2018.
[34] Willem van de Wiele, 'European FinTech: New Rules on the Way' (2018) 37 (5) Banking & Financial Services Policy Report 16, 18.

independent existence of virtual currencies, such as Bitcoin, a "record of the money in all of the accounts would enable to follow the movements, establishing a verification mechanism."[35]

Moreover, close cooperation with the private sector further strengthens financial stability. In February 2018, seven companies from the UK established a self-regulatory body CryptoUK who developed a code of conduct. For policy makers this step is significant as it helps the development of broader UK rules around volatile cryptocurrency trading.[36]

The problem in ensuring data protection. At this stage, it is not clear how decentralised blockchain networks will be able to adequate ensure data protection, to implement all of standards envisaged by the General Data Protection Regulation. As rightly put by Robert Herian, a "key question remains the matter of control of the personal data and the accountability for the administration of the blockchain application within the scope of the GDPR."[37] A close follow up with the findings of the European Blockchain Partnership will help to identify how to fulfil the obligations under the GDPR without stifling innovation.

Regulating digital currencies: lessons from overseas

Other jurisdictions have either put cryptocurrencies into a specific legal category or developed a new regulatory framework dealing with virtual currencies. While Germany regulates exchanges using existing anti-money laundering laws, the US is supporting legal changes in order to accommodate the law with the risks connected with virtual currencies.[38] The UK is preparing to regulate in this area. The recent statement of the Governor of the Bank of England, Mark Carney, is indicative that it is necessary to "bring crypto-assets onto a level regulatory playing field in order to combat illicit activities, promote market integrity, and protect the safety and soundness of the financial system."[39]

A possibility is to follow the approach taken in Germany, classifying cryptocurrencies as financial instruments. In Germany, digital currencies are classified without distinction of the software they are

---

[35] Andres Guadamuz and Chris Marsden, 'Blockchains and Bitcoin: Regulatory responses to cryptocurrencies' (*FirstMonday: Peer-reviewed journal on the Internet*, 7 December 2015) < http://firstmonday.org/article/view/6198/5163> accessed 7 October 2018.
[36] Thomas Delahunty, 'Seven Crypto Companies Form UK Cryptocurrency trade body Crypto UK' (*NewsBT*, 13 February 2018) < https://www.newsbtc.com/2018/02/13/cryptouk-crypto-companies-form-uk-cryptocurrency-trading-body/> accessed 7 October 2018.
[37] Robert Herian, 'Regulating Disruption: Blockchain GDPR and Questions of Data Sovereignty' (2018) 22 (2) Journal of Internet Law 7, 13.
[38] FAFT, 'Guidance For A Risk-Based Approach Virtual Currencies' (June 2015) < http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 5 October 2018 at [85]- [87].
[39] 'BoE Governor Speaks on the Need to Regulate Crypto Assets' (Moody's Analytics, 2 March 2018) <https://www.moodysanalytics.com/regulatory-news/mar-02-18-boe-governor-speaks-on-the-need-to-regulate-crypto-assets> accessed 8 October 2018.

based on or the encryption technologies that apply. The Germany Federal Financial Supervisory Authority ("BaFin") decided that cryptocurrencies that possess the character of a cash instrument are defined as "financial instruments" under section 1 (11) sentence 1 the Germany Banking Act. Units of account are treated similar to foreign exchange, with the difference that they do not refer to a legal tender. Because virtual currencies do not constitute legal tender, they are not qualified as currency, banknotes or coins in accordance with the *Zahlungsdiensteaufsichtsgesetz* (German Payment Services Supervision Act). However, any business carried out by e-money, that is any digital means of payment supported by a central entity issuing the units, will fall under section 1 of the German Payment Services Supervision Act.

The dealings with virtual currencies do not require an authorisation requirement under German banking laws, unless the actions are classified as commercial dealings. This means that the use of virtual currencies as a means of deposit to conduct exchange transactions or as a substitute for cash does not require authorisation. A license of the BaFin is also not required for the mining of virtual currencies, because the digital currencies are not issued, nor placed by the miners themselves. Finally, the purchase or the sale of virtual currencies does not require authorisation.

As a result, the use of virtual currencies as a payment for goods and services as a means of exchange transactions will fall under Anti-Money Laundering regulation. The German Money Laundering Act (transposing the MLD4 AML requirements) becomes applicable in instances where there is a commercial dealing, triggering an authorisation requirement.

The Austrian financial services regulatory body takes the approach that cryptocurrencies are currently neither treated as financial instruments nor as currency but as commodities. However, although commodities are not subject to supervision by the FMA, business activities involving cryptocurrencies are still within the Austrian regulatory regime. The operation of various business models based on cryptocurrencies may trigger licensing requirements under the Austrian Banking Act (BWG; Bankwesengesetz), the Austrian Alternative Investment Fund Manager Act (AIFMG; Alternative Investmentfonds Manager-Gesetz), the Austrian Payment Services Act (ZaDiG; Zahlungsdienstegesetz) and/or the prospectus requirements under the Austrian Capital Markets Act (KMG; Kapitalmarktgesetz).

Austria has introduced regimes for the taxation of cryptocurrencies. Income generated from cryptocurrencies may also be taxable in Austria (depending on the value of income generated). The world's first Bitcoin Bank has opened in Vienna. The ATM machines exchange bitcoin for Euro, and vice versa. Where cryptocurrency has been exchanged into fiat currency (eg Euro) and vice versa,

VAT is exempt (CJEU 22 Oct 2015, C-264/14, Hedquvist). Vienna now has more than 20 bitcoin friendly vendors ranging from restaurants, bistros and bars. Payments made in cryptocurrency for the purchase/supply of goods or services that are subject to VAT are treated no differently from payments made with fiat currency.

The Australian Transaction Reports and Analysis Centre (Austrac) has proposed the introduction of measures similar to those in Japan which stipulate that crypto-currency exchanges must conduct annual audits and comply with the same Know Your Customer and Anti-Money Laundering rules applied to traditional exchanges and institutions, following a recent scandal involving the Commonwealth Bank of Australia (CBA) who were relaxed about rules regarding anti-money laundering and terrorist financing. The proposed legislation has been welcomed by the Australian Digital Currency & Commerce Association which said it will increase safeguards and provide regulatory certainty to digital currency businesses.

Japan was the first national government to grant virtual currencies full legal status as a payment method, prompted by the 2014 bankruptcy of Mt Gox, the world's largest virtual currency exchange.

A considerable effort to establish a framework around cryptocurrencies has been done by the US. As indicated by Internal Revenue Service, virtual currencies are treated as property for taxation purposes. In a letter in 2018 published by the Financial Crimes Enforcement Network it has been stated that token issuers and exchanges are classified as “money transmitters” which requires them to register and comply with anti-money laundering laws and the know-your-customer rules. As a result, the US regulates any legal or natural person’s activities which involve accepting convertible digital currencies, defining convertible virtual currency exchangers and administrators as money transmitters.[40]

The tight regulation of cryptocurrencies should have a signalling effect to develop a powerful framework that mitigates risks of financial crime. In 2014, the New York State Department of Finance proposed a BitLicense regulatory framework, which should be implemented by businesses in their dealings with virtual currencies.[41] The framework contains an anti-money laundering program, a cyber-security program and rules on consumer protection for firms using virtual currencies in the State

[40] FAFT, ‘Guidance For A Risk-Based Approach Virtual Currencies’ (June 2015) < http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 5 October 2018 at [86].
[41] Octavian Nica, Karolina Piotrowska, Klaus Reiner Schenk-Hoppe, ‘Cryptocurrencies: Economic benefits and risks’ (University of Manchester FinTech working paper no 2, 26 October 2017) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3059856> accessed 5 October 2018 at page 32.

of New York.[42]

Conclusion:

The findings of this collaborative essay are intended to underline the modern threats of the use of virtual currencies with regard to money laundering, financial crime, cyber security and terrorist financing. Understanding the risks is imperative to develop a robust regulatory framework which is able to strike the right balance between safeguarding the business and consumer interests as well as maintaining innovation. Focusing on the UK, the findings of this investigation suggest that the implementation of the 5th Money Laundering Directive will ensure the level of regulatory oversight over the use of digital currencies.

[42] New York State Department of Financial Services, 'New York Codes, Rules and Regulations – Chapter I: Regulations of the Superintendent of Financial Services Part 200: Virtual Currencies' (6 February 2015) < https://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf> accessed 8 October 2018.