Title: Legal Regulation of Virtual Currencies: Illicit Activities and Current Developments in the Realm of Payment Systems

Author: Ilias Ioannou

Source: *The King's Student Law Review*, Vol XI, Issue I

Published by: King's College London on behalf of The King's Student Law Review

---

Legal Regulation of Virtual Currencies: Illicit Activities and Current Developments in the Realm of Payment Systems

Ilias Ioannou

Since Bitcoin was invented a decade ago, the phenomenon of Virtual Currencies has been hailed as an ingenious innovation and decried as the preferred transaction vehicle for illicit actors. Despite the numerous headlines discussing the virtues and vices of virtual currencies, heretofore there has been no comprehensive legal response. The present contribution elaborates on the regulation of virtual currencies in the European Legal Area. Starting with a conceptual analysis of virtual currencies and their promising potential, it identifies the financial crime risks posed by the intersection between legitimate and illegitimate users. The research shows that a fragmentary regulation would be ineffective; this promising technology will either be integrated into the lawful economy or it will be exploited by criminals. The paper attempts to fill the regulatory gap by providing a recommendation for the embeddedness of Virtual Currencies into the financial system. It achieves that by redirecting regulation towards the uniqueness of their underlying technology.

Introduction

Virtual Currencies (VCs) present exceptional opportunities for innovation and development in international payment and remittance systems. They offer 'a version of electronic cash' that allows 'online payments to be sent directly from one party to another without going through a financial institution.'[1] Ongoing initiatives, such as Facebook's *Libra*, aspire to bring cryptocurrency to the masses by providing 'a reliable digital currency and infrastructure that together can deliver on the promise of the internet of money.'[2] However, VCs are also uniquely tailored to facilitate illegitimate activities. Starting with an analysis of the applicability and suitability of the current European Union (EU) legal concepts, this inquiry will re-examine the statutory framework for the regulation of companies engaging in virtual currency business

[1] Satoshi Nakamoto, 'Bitcoin: A Peer to Peer Electronic Cash System' (Bitcoin, 2008) <https://bitcoin.org/bitcoin.pdf> accessed 16 December 2019.

[2] Libra Association, 'An introduction to Libra', (Libra, 2019), 4 <https://libra.org/en-US/white-paper/?noredirect=en-US#introduction> accessed 16 December 2019.

activity. In the current state of affairs, where the Fifth Anti-Money Laundering Directive[3] has to be implemented by member states into national law, this research could function as an inquiry on its implementation.

Following an introductory chapter on the basic notions related to VCs, Part 2 analyses their promising role in the realm of international payments. Subsequently, in Part 3, the illicit activities are identified through a risk analysis method in the context of money laundering, terrorist financing and illicit flow of money. It is argued that regulation needs to be balanced between the attractiveness of VCs and the identified financial crime risks. To that effect, Part 4 analyses the extent at which VCs are currently regulated under the existing EU regulatory framework. In Part V the inadequacy of the existing framework is highlighted and concrete recommendations for law reform are laid out. The article concludes with a comprehensive proposition for the legal regulation of VCs on the basis of their underlying technology.

1. Typology of Virtual Currencies

1A: Key Definitions

As regulators around the globe begin to deal with the legal challenges that VCs pose to the payment systems, it becomes clear that they lack a common language that accurately describes the different types of VCs.[4] In the EU, the Fifth Anti-Money Laundering Directive (hereinafter 5AMLD) legally defines VCs as follows:

> A digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.[5]

---

[3] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L 156/43.

[4] Robby Houben and Alexander Snyers, 'Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion' (July 2018) Department for Economic, Scientific and Quality of Life Policies, 20 <https://goo.gl/PSxbzx> accessed 5 April 2020.

[5] See art.1(2)(d) of the 5AMLD, which inserts this definition in the art.3(18) of the Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing [2015] OJ L 141/73 (hereinafter 4AMLD).

According to the Financial Action Task Force (FATF) virtual currency is 'a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status in any jurisdiction'.[6] The legal tender status refers to monetary instruments that, by law, can be used by a debtor of a monetary debt to discharge the debt, without necessarily requiring the creditor to accept the payment.[7] The term is used in this article broadly to refer to cryptocurrencies, stablecoins, virtual tokens and other altcoins,[8] that can be used as a means of payment without having a legal tender status.

1B: Taxonomy

Regarding their functionality as tokens, virtual assets have been distinguished by legislative authorities and commentators into three classes:[9] (i) 'exchange' or 'currency' tokens, which are intended and designed to be used as a means of exchange, (ii) 'utility tokens', which, akin to pre-payment vouchers, embody a relationship between the token issuer and the token holder, and (iii) 'security' or 'investment' tokens, which are comparable to traditional securities. The research hereinafter focuses primarily on the first kind of tokens, which are the most relevant to the payment industry.

Exchange tokens can be analysed further into cryptocurrencies, stablecoins and e-money tokens. The term cryptocurrency is commonly understood as a specific

---

[6] FATF, 'Virtual Currencies: Key definitions and Potential AML/CFT Risks' (June 2014), 4 <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 16 December 2019.

[7] See Commission Recommendation 2010/191/EU on the scope and effects of legal tender of euro banknotes and coins [2010] OJ L 83/70, which refers to three characteristics of legal tender: (1) it is mandatory acceptance; (2) its acceptance at full face value; and (3) its power to discharge payment obligations. Similarly, in English law, the concept of legal tender developed from the law on the performance of debts; See Moss v Hancock (1899) 2 Q.B. 116; See also Thomas H Greco, 'Money: Understanding and creating alternatives to legal tender', (Chelsea Green Publishing 2001) 26.

[8] 'Altcoin' is a combination of the word 'alt' signifying 'alternative' and 'coin' signifying 'cryptocurrency'. Thus, it refers to all cryptocurrencies which are alternatives to the first cryptocurrency, namely all cryptocurrencies which are not Bitcoin.

[9] FCA, 'Guidance on Cryptoassets' (July 2019) <https://www.fca.org.uk/publication/policy/ps19-22.pdf> accessed 16 December 2019; Philipp Maume and Mathias Fromberger, 'Regulation of Initial Coin Offerings: Reconciling US and EU Securities Laws' (2019) 19 (2) Chicago Journal of International Law 548, 558; Luka Muller et al, 'Conceptual Framework for Legal and Risk Assessment of Crypto Tokens' (Zurich 2019), 10 <https://www.mme.ch/fileadmin/files/documents/180501_BCP_Framework_for_Assessment_of_Crypto_Tokens_-_Block_2.pdf> accessed 16 December 2019.

subcategory of VCs, namely 'decentralised convertible VC that is protected by cryptography'.[10] A stablecoin is a token designed to avoid the volatility inherent in other VCs by using a variety of mechanisms.[11] Lastly, e-money is usually understood as a digital transfer mechanism for fiat currency,[12] and it is distinct from digital currency which is an overarching term for digital representation of either VC or fiat money.

1C: Blockchain System Participants

Various actors are involved in the VC ecosystem. A first player is the issuer of a VC, which can be either the 'coin inventor' or 'coin offeror'.[13] A coin inventor is an individual or an organisation that sets up the technical foundations of a VC and gratuitously distribute it. A coin offeror offers the token at an initial coin offering (ICO) against payment.[14] A second player consists of VC exchanges, which are businesses engaged in the exchange of VCs for fiat currency, funds or other VCs and vice versa for a commission.[15] The so-called 'trading platforms' comprise another possible entry-point to the VC market, as they provide users with a platform on which they can directly trade with each other online or even locally.[16]

To purchase, hold and transfer VCs, end-users need a pair of cryptographic keys. This pair of private and public keys allows the user to transfer VCs in the form of transaction outputs/inputs, which are stored in a 'wallet' that is the primary user's

---

[10] FATF, Virtual Currencies 2014 (n 6) 5.

[11] Makiko Mita, Kensuke Ito, Shohei Ohsawa and Hideyuki Tanaka, 'What is Stablecoin?: A Survey on Price Stabilisation Mechanisms for Decentralised Payment Systems' (2019), 2 <arXiv:1906.06037v1> accessed 16 December 2019. According to Regnard-Weinrabe, these mechanisms include fiat/asset-collateralised, crypto-collateralised and non-collateralised stabilisation models. See Ben Regnard-Weinrabe, 'Stablecoins' (Harvard Law School Forum on Corporate Governance and Financial Regulation, 10 February 2019) <https://corpgov.law.harvard.edu/2019/02/10/stablecoins/> accessed 16 December 2019.

[12] The so-called 'fiat currency' is any currency that exists and has a nominal value determined by the law establishing the currency. According to FATF, 'Virtual Currencies: Guidance for a risk-based approach' (June 2015) 26, 'fiat currency' is 'the coin and paper money of a country that is designated as legal tender; circulates and is customarily used and accepted as a medium of exchange'. The 5AMLD defines fiat currency more broadly as 'coins and banknotes that are designated as legal tender and electronic money of a country.'

[13] Houben and Snyers (n 4) 28.

[14] For an overview of the ICO market, see Dirk Zetzsche et al., 'The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators', (2019) 63 Harvard International Law Journal, 2 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3072298> accessed 16 December 2019.

[15] FATF, Virtual Currencies 2014 (n 7) 7.

[16] For example, www.localbitcoins.com.

interface.[17] A wallet provider translates an address transaction history into a customer friendly format, enabling end-users to conduct VC transactions.[18] Wallet providers can be distinguished between custodian and non-custodian. Custodian wallet providers run platforms which allow users to create accounts and automatically store their private keys. To perform a transaction, the sender only needs to access credentials similar to an e-banking platform and is not required to remember their private key. In contrast, non-custodian wallet providers facilitate end-users to store their private keys themselves by providing them with a suitable wallet.[19]

Finally, the so-called 'tumbler services',[20] a different type of service provider, amalgamates a VC transaction with others to obscure the nexus between a sender and a recipient.[21] In this way, it becomes unclear whom the user intended the VCs to be directed to. Skillful users may use other tools designed to further enhance online anonymity, such as *Tor*[22] and *Darkwallet*.[23]

The conceptual tools elaborated in this chapter will serve as a benchmark throughout this paper and will facilitate the assessment of the adequacy of the existing and upcoming legal framework. Before touching upon the details of how regulation needs to be reoriented, the study will examine the revolutionising potential of VCs in the context of payment systems.

---

[17] Andreas Antonopoulos, *Mastering Bitcoin* (2nd Edition O'Reilly 2018) Ch. 5.
[18] Houben and Snyers (n 4) 27.
[19] For example, a hardware wallet (USB device) or a paper wallet (a piece of paper with two QR codes on it).
[20] For example, https://bitblender.io/ or https://bitcoin-laundry.com/
[21] Lars Haffke, Mathias Fromberger and Patrick Zimmermann, 'Virtual Currencies and AML – The Shortcomings of the 5th AML Directive (EU) and How to Address Them' (2019), 7 <papers.ssrn.com/sol3/papers.cfm?abstract_id=3328064;> accessed 16 December 2019.
[22] Tor (www.torproject.org/download/) is a network that permits users to browse the web anonymously. See Husam Al Jawaheri, Mashael Al Sabah, Yazan Boshmaf and Aiman Erbad, 'Deanonymising Tor hidden service users through Bitcoin Transactions analysis' (2020) 89 Computers & Security <https://www.sciencedirect.com/science/article/pii/S0167404818309908?A> accessed 5 April 2020.
[23] Dark wallet is a digital wallet which promises total anonymity to its user base. See Aaron Van Wirdum, 'CoinJoin's First Steps: How Dark Wallet Paved the Way for A More Private Bitcoin' (Bitcoin Magazine, February 2020) < https://bitcoinmagazine.com/articles/coinjoins-first-steps-how-dark-wallet-paved-the-way-for-a-more-private-bitcoin> accessed 5 April 2020; Cath Senker, *Cybercrime and the Darknet: Revealing the hidden underworld of the Internet* (Arcturus Publishing 2016); Sesha Kethineni, Ying Han Cao and Casssandra Dodge 'Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes' (2018) 43(2) American Journal of Criminal Justice, 141.

2. The Promising Role of Virtual Currencies in International Payment Systems

2A: The Status Quo and Fintech Solutions

A payment is considered to be 'any act offered and accepted in performance of a money obligation'.[24] In a simple credit transfer scheme, various intermediaries could be involved, such as the debtor's bank, the corresponding bank, intermediary banks, interbank correspondents, international clearing agents and central settlement/clearing institutions. The validation of information at each intermediary is timely, costly and the associated transaction risk is concentrated in large clearing houses. According to the Federal Reserve, the cental bank of the United States, the risks that may arise include the credit or counterparty risk, liquidity risk, operational risk and the legal risk.[25] To balance those risks, banks impose high transaction and remittance costs to the consumers.

In this context, there have been remarkable developments for the cross-border transfers of money. For example, *TransferWise* performs international transfers through two local transfers linked together by software. Similarly, *Revolut*, an entirely digital bank with minimal operational expenditure, can hold and exchange with the interbank exchange rate 29 currencies, including 5 VCs. Overall, the payment industry has attracted a spate of fintech start-up businesses, such as *Stripe, Alipay, Moneygram* and *M-Pesa*, which facilitate transactions denominated, primarily, in fiat money.[26] The process of modernisation and digital transformation of current payment systems creates fertile ground for the adoption of new technologies, such as blockchains and more generally distributed ledger technologies.[27]

2B: Permission-less Blockchain Payment Systems

The most famous permission-less blockchain-based payment system is Bitcoin. According to Antonopoulos, 'bitcoin is a collection of concepts and technologies that form the basis of a digital money ecosystem'.[28] A key characteristic of Bitcoin is that it is entirely virtual and that there are no physical or even digital coins *per se*. The users

[24] Ewan McKendrick, *Goode on Commercial Law* (5th ed. 2016), 488.
[25] Federal Reserve, 'Policy on Payment System Risk', 2017, 4-5.
[26] Ignacio Mas and Dan Radcliffe, 'Mobile Payments Go Viral: M-PESA in Kenya' (2011) 32 Journal of Financial Transformation 169.
[27] Anton Didenko and Ross Buckley, 'The evolution of currency: From Cash to Cryptos to Sovereign Digital Currencies' (2019) 42 (4) Fordham International Law Journal 1041, 1070.
[28] Antonopoulos (n 17) 1.

have their own keys and can participate in the network as full node validators of the transactions. The transactions are peer-to-peer and there is not a central clearing house or point of control. The disintermediation of the payment system results in much lower transaction fees and, theoretically, there are no transaction or foreign exchange risks.

On the other side of the spectrum, significant price fluctuations[29] and scalability issues have prevented permission-less blockchain-based VCs from being broadly accepted. As permission-less VCs transform to speculative assets, their utility as decentralised payment mechanisms become secondary. That is one of the reasons for the shift towards stablecoin proposals running in permissioned blockchains, such as *Libra*[30] in the retail payments context and the *JPM coin* in financial markets. [31]

2C: Permissioned Blockchain Payment Systems

Permissioned blockchains maintain an access control layer to allow certain actions to be performed solely by authorised participants.[32] In terms of payment systems, a permissioned blockchain could be a peer-to-peer network of participating banks or private institutions. The latter will act as validators of the transactions and not as classical intermediaries. Following network validation, native tokens, which could be stablecoins, are transferred between the counterparties. The difference from a permission-less blockchain is that the counterparties can either be the permissioned entities, in which case the blockchain is used as a settlement mechanism, or 'lightweight clients', whereby the transaction will take place directly between wallet holders and/or end-users but will be validated only by the participating banks or authorised entities that operate as full nodes.[33]

Blockchain-based VCs make possible to transfer value across the globe in a seamless and cost-effective way. The counterparty risk, the liquidity risk, the operational risk as well as the legal ambiguities associated with the current payment infrastructure are eliminated by the instantaneous transfer of ownership. Similarly, the high transaction costs and the geographical limitations of Fintech-based payment systems could be

---

[29] Gina Pieters and Sofia Vivanco, 'Financial regulations and price inconsistencies across Bitcoin markets' (2017) 39 Information Economics and Policy 3.
[30] See Libra Association (n 2) 4.
[31] Press Release, 'J.P. Morgan Creates Digital Coin for Payments' (February 2019) <https://www.jpmorgan.com/global/news/digital-coin-payments> accessed 16 December 2019.
[32] Jake Frankenfield, 'Permissioned Blockchain' (Investopedia, August 2019) <https://www.investopedia.com/terms/p/permissioned-blockchains.asp> accessed 16 December 2019.
[33] For a comparison of blockchain protocols see Taskinsoy, 'Facebook's Project Libra' (2019) 14 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3423453> accessed 16 December 2019.

supplanted by fast, scalable and secure global VCs. However, the lack of a definite legal framework and the risks associated with the use of VCs have prevented their promising role from coming to fruition.

3 Risks Associated with the Use of Virtual Currencies

3A: Understanding Financial Crime Threats

VCs have the potential to offer benefits to businesses and consumers, but they also have features which make them attractive for abuse, namely, their almost anonymous nature, their global reach and the absence of a central intermediary.

High Level of Anonymity

The foundational cause that provokes illicit activities using VCs is the high level of anonymity associated with them. Anonymity can be construed both as privacy and hidden identity.[34] Anonymity as privacy refers to citizenry concerns regarding their personal data and their freedom to browse the web and make purchases without being tracked. As such, privacy is considered a desirable feature of VCs.[35] In contrast, anonymity as hidden identity is affiliated with criminals who need it to avoid the authorities and hide their identity.[36] Given that anyone can create as many public addresses as they want without providing any identifying information, some VCs enable completely anonymous transfers.[37]

It should be noted, however, that most VCs are not entirely anonymous. Instead, they are pseudonymous, and the owners are identified by their public cryptocurrency address. Consequently, given that the identity of some wallet owners is known, it is possible to use these known addresses in order to track the transactions.[38] By doing so, law enforcement agencies can deploy techniques to expose the identity of the owners of unknown wallets with whom the known wallets transacted.[39] This could create a

[34] Victor Dostov and Pavel Shust, 'Cryptocurrencies: an unconventional challenge to the AML/CFT regulators?' (2014) 21(3) Journal of Financial Crime 249, 258.
[35] Ibid.
[36] Gary Marx, 'Identity and Anonymity: Some Conceptual Distinctions and Issues for Research' in J Caplan and J Torpey (eds), *Documenting Individual Identity* (Princeton University Press, 2001) 311.
[37] David Carlisle, 'Virtual Currencies and Financial Crime', RUSI Occasional Paper, (March 2017) 10.
[38] For example, *Chainanalysis Inc*. has developed an adequate software to track Blockchain transactions.
[39] Steven Goldfeder et al., 'When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies' (CoRR 2017), 2-3 <https://arxiv.org/pdf/1708.04748.pdf> accessed 16 December 2019.

cascade effect, whereby the increase of identified wallet holders would make it easier to identify the owners of unknown addresses.[40] For this reason, reform of the regulation should be in line with an approach toward gathering as much information as possible for the enforcement authorities.

Absence of a Central Intermediary

Depending on their issuance and administration pattern, VCs can be either centralised or decentralised.[41] All closed and unidirectional VCs are centralised because they are issued by a central entity.[42] Decentralised VCs are distributed open-source, peer-to-peer and have no central administering authority.[43] This means that the entire system is made up 'of versions of the software that end-users download and run on their personal computers.'[44]

In this regard, a second reason that renders decentralised VCs suitable for illicit activities is that the existing financial regulation system relies on regulating intermediaries to control harmful behaviour. For instance, financial institutions are used as regulatory agents and are obliged to perform know-your-customer (KYC) and other customer due diligence (CDD) duties to prevent money laundering.[45] In the context of VCs, miners, exchanges, wallet providers and other system participants are indispensable in enabling blockchain payment networks to function. However, payment systems operating on permission-less blockchain are still decentralised and anyone can participate on a peer-to-peer basis. As a result, law enforcement authorities cannot target a central administrator or clearing house for investigative and law

[40] Omri Marian, 'A conceptual framework for the regulation of cryptocurrencies' (2015) 82 University of Chicago Law Review Dialogue 53, 63.
[41] ECB, 'Virtual Currency Schemes – A further analysis' (2015), 6 <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> accessed 16 December 2019.
[42] FATF, Virtual Currencies 2014 (n 6), 5.
[43] Angela Walch 'The Bitcoin Blockchain as Financial Market Infrastructure: A consideration of Operational Risk' (2015) 18(4) NYU Journal of Legislation & Public Policy, 33.
[44] Shawn Bayern, 'Of Bitcoins, Independently Wealthy Software, and the Zero-Member LLC' (2014) 108 Northwestern University Law Review 1485, 1488 <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1009&context=nulr> accessed 16 December 2019.
[45] Andy Yee, 'Internet Architecture and the Layers Principle: A conceptual framework for regulating Bitcoin' (2014) 3(3) Internet Policy Review 3.

enforcement purposes.[46] Therefore, it is crucial to identify which players in the VC market should be regulated.[47]

Global Reach

Lastly, a key innovation of VC systems is their worldwide accessibility through the Internet and their ability to transcend national borders instantaneously. However, the inherently cross-border and mobile nature of VCs likewise makes them well suited for transnational crimes. Particularly, some participants of a decentralised VC ecosystem may be located in jurisdictions that do not have effective regulations or adequate AML/CFT controls, thereby leveraging completely anonymous interaction with the system.[48] Similarly, with regard to VCs that are deployed in permissioned blockchains, other actors could consciously seek out jurisdictions with weak AML controls to engage with money laundering schemes or to avoid the costs of compliance.[49] During subsequent stages, the VCs can be freely transferred across borders between different wallets in any other country. To create a level playing field and prevent 'a potential race to the bottom' by different States[50] and forum shopping by different system participants, regulation will only be adequate when it is adopted at a supranational or even global level.

Financial Crime Risk Analysis Methodology

The aforementioned characteristics not only enable end-users to disguise the source and purpose of money, making VCs appealing for money launderers and terrorist financiers, but they can also act as a payment mechanism between criminals.

In this context, it has been suggested that, before committing a crime, prospective criminals consider both the expected outcome from their criminal action as well as the probability and cost of any penalty that may be levied upon them.[51] Following this, they decide whether it is in their interest to engage in a particular crime.[52] Using VCs

---

[46] Loretta Michaels and Mathew Hommer, 'Regulation and Supervision in a Digital and Inclusive World' in David Kuo Chuen and Robert Deng (eds), *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1* (Elsevier Academic Press 2018).
[47] Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Cambridge, Harvard Press 2018), 6
[48] FATF, Virtual Currencies 2014 (n 6) 10.
[49] Haffke, Fromberger and Zimmermann (n 21) 5.
[50] Ibid 10.
[51] This is the classic utility model of criminal behaviour suggested by Gary S Becker at 'Crime and Punishment: An Economic Approach', (1968) 76(2) The Journal of Political Economy 169, 177.
[52] Becker's basic utility model is defined as:

as a vehicle for nefarious activity significantly reduces the probability of detection due to the related anonymity. The reduced likelihood of being caught respectively decreases the deterrence factor. Therefore, in the absence of a regulatory response, the introduction of VCs would reasonably be expected to increase the level of criminal activity *ceteris paribus*, because more individuals would choose to engage in it.[53]

Admittedly, such unlawful behaviour also exists in the fiat payment system. Credit cards, e-banking, wire transfers and cash transactions all continue to be exploited for illicit activities.[54] Accordingly, the legal regulation of VCs should not necessarily aim to eliminate the interconnected financial crime risks. If that was the only concern of the European regulator, then a complete prohibition of VCs would be justified.[55] Instead, the regulation should inhibit the additional risks emerging from the specific features of VCs without preventing VCs from achieving their innovative potential. Consequently, it is necessary to only target the anonymity, disintermediation and cross-border nature of VCs to the extent that they limit the current level of criminal activity.[56]

3B: The Use of Virtual Currencies for Illicit Activities

The anonymity risks, in conjunction with the absence of sufficient regulation, instigate the offender's motive and abet the following types of criminality.

Money Laundering

VCs are notoriously used to launder the proceeds of crime through two recognisable methods. Firstly, dirty fiat currency are converted into VCs and then put through a variety of transfers to obscure the fund's illegal source.[57] Unlicensed entities, including VC exchanges, peer-to-peer trading platforms and tumbling services can be used to introduce illegal gains into the VC ecosystem as a result of the absence of strict KYC and other suspicious activity reporting (SAR) measures that financial institutions

$$E[U] = pU(Y-f) + (1-p)\,U\,(Y)$$

Where EU is the expected utility from engaging in criminal behaviour; p is the probability of conviction per offence; Y is the income expected to be generated from an offence; and f is the monetary equivalent of the criminal sanction. See Ibid.

[53] Marian (n 40) 60.

[54] Yaya J. Fanusie and Tom Robinson, 'Bitcoin laundering: an analysis of illicit flows into digital currency services' (2018) Centre on Sanctions & Illicit Finance, 13.

[55] Complete prohibition was the legal approach to VCs in some countries, such as Bangladesh, Bolivia, and Thailand. See Michael Sackheim and Nathan Howell (eds) *The Virtual Currency Regulation Review* (The Law Reviews 2018) 243.

[56] Marian (n 40) 59.

[57] Carlisle (n 37) 14.

usually implement. Criminal counterparts can then complete the placement stage of money laundering and hide the nexus between the VCs and their origin.[58] A second *modus operandi* involves perpetrators selling illegal goods or services directly in exchange for VCs and subsequently converting those to fiat currency.

Law enforcement is already seeing cases of money laundering exploiting both centralised and decentralised VCs. The most famous case involving a centralised VC is the case of *Liberty Reserve*,[59] which is considered one of the largest online money laundering cases in history.[60] *Liberty Reserve* was an Internet-based payment system which issued its own VC and purposely assisted money laundering among criminals.[61] The VC, liberty dollar, was a bidirectional stablecoin and the transfers were denominated and stored in US dollars.

Among decentralised VCs, an important ongoing money laundering case is the indictment of 'BTC-e' and its executive Alexander Vinnik[62] for the alleged crimes of conspiracy, money laundering and operating an unlicensed exchange.[63] The most notorious money laundering case, however, is the *Silk Road*, a cryptomarket[64] designed to enable its users to sell and purchase illegal goods and services. Its creator, Ross Ulbricht, was convicted *inter alia* of money laundering and sentenced to life imprisonment.[65] Other well-known cases include the VC exchanges *BitInstant*,[66]

---

[58] The process of Money Laundering involves three recognisable phases: placement, layering and integration. See Jeffrey Simpser, 'Money Laundering and asset cloaking techniques' (2008) Journal of Money Laundering Control 15; Stefan Cassella, 'Toward a New Model of Money Laundering: Is the 'Placement, Layering, Integration' Model Obsolete?' (2018) 21 Journal of Money Laundering Control 494.

[59] Press Release, US DoJ, 'Co-founder of Liberty Reserve Pleads Guilty to Money Laundering' (2013) <http://www.justice.gov/opa/pr/2013/October/13-crm-1163.html> accessed 16 December 2019.

[60] According to Carlisle (n 37) 15, the value of the transactions involved is estimated at 8bn USD.

[61] Lawrence Trautman, 'Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?' (2014) 20(4) Richmond Journal of Law & Technology 87 <http://jolt.richmond.edu/v20i4/article13.pdf> accessed 16 December 2019.

[62] Indictment *US v BTC-e and Alexander Vinnik*, case 4:19 US District Court Northern District of California <https://www.scribd.com/document/419868940/US-vs-BTC-e-Vinnik> accessed 16 December 2019.

[63] Daniel Kuhn, 'Prosecutors file formal complaint against infamous BTC-e crypto exchange' (CoinDesk, July 2019) <https://www.coindesk.com/formal-complaint-filed-against-infamous-btc-e-exchange> accessed 16 December 2019.

[64] See *infra* 3B § 3.

[65] *U.S. v Ulbricht*, 2014 US District LEXIS 93093.

[66] Jose Pagliery, 'Bitcoin Exchange CEO Arrested for Money Laundering' CNN Tech (January 2014) <https://money.cnn.com/2014/01/27/technology/security/bitcoin-arrest/index.html> accessed 16 December 2019.

OKCoin,[67] where hundreds of thousands of US dollars were laundered, and *Ripple*, where a 700,000 USD civil penalty was levied to Ripple Labs Inc. for failure to maintain an adequate AML programme.[68]

Terrorist Financing

The rise of the Islamic State (IS), also known as Daesh, ISIS or ISIL, has raised concerns that terrorist organisations could deploy VCs to finance deeds of terrorism.[69] Specifically, it has been argued that the aforementioned characteristics of VCs make them 'ideal for terrorism financing'.[70] However, law enforcement actions against terrorist financiers who employ VCs are limited and largely anecdotal. In the US, an adolescent male was sentenced to more than 11 years for using a Twitter account to describe how to support the IS with *bitcoin*.[71] In Indonesia, authorities have claimed that IS militants have used PayPal and *bitcoin* for money transfers. However, they did not share further details.[72] Generally, terrorist actions seem to require simpler forms of funding and terrorist financing through VCs ought to be regarded as a potential risk, rather than a crystallised one.[73]

Cryptomarkets

Cryptomarkets, such as the infamous drug marketplaces *Silk Road* and *AlphaBay*, are online platforms designed to facilitate the trade of illicit commodities. They provide their participants with anonymity as they are located on the dark web and they utilise cryptocurrencies for payment. The most tradeable products in cryptomarkets include

---

[67] Gautham, 'Bitcoin Exchange OKCoin Fined in Money Laundering Case' (newsbtc, 2016) <https://www.newsbtc.com/2016/08/15/china-okcoin-exchange-fined/> accessed 16 December 2019.

[68] Press Release, 'FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger' (2015) <https://www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual> accessed 16 December 2019.

[69] Alan Brill and Lonnie Keene, 'Cryptocurrencies: The Next Generation of Terrorist Financing?' (2014) 6(1) Defence Against Terrorism Review 7.

[70] Iwa Salami 'Terrorism Financing with Virtual Currencies' (2018) 41 (12) Studies in Conflict &Terrorism, 968, 971.

[71] Press Release, US DoJ, 'Virginia man sentenced to more than 11 years for providing material support to ISIL' (2015) <https://www.justice.gov/opa/pr/virginia-man-sentenced-more-11-years-providing-material-support-isil> accessed 16 December 2019.

[72] Pete Rizzo, 'Indonesia's AML watchdog links bitcoin to IS' (CoinDesk, January 2019) <https://www.coindesk.com/indonesias-aml-agency-links-bitcoin-islamic-state-terrorism> accessed 16 December 2019.

[73] See Europol, 'Changes in Modus Operandi of Islamic State Terrorist Attacks', (January 2016) 7.

illegal drugs, stolen information, weapons, pornographic content and other illicit services, such as hacking for hire.[74]

It should be noted however that cryptomarkets anonymity is not achieved by VCs *per se*. Instead, end-users obfuscate their IP addresses and encipher their communication by operating on the Tor network and utilising encryption software. The role of VCs is restricted as a means of payment. As explained above, the pseudonymous nature of well-known VCs empowers authorities to relate transactions and pinpoint the identity of the owner of an address. This became evident in the *Silk Road* case where the arrest of Ulbricht enabled law enforcement to track illegal transactions and identify a number of participants including his employees,[75] drug traffickers,[76] *bitcoin* vendors[77] and the FBI agents who initially investigated and blackmailed him.[78]

To achieve complete anonymous transactions, participants in cryptomarkets usually prefer to use altcoins of enhanced privacy, as for example *Dash*, *Monero (XMR)*, *NEO* and *DarkCoin (DARK)*.[79] These VCs are not usually available in virtual-to-fiat currency exchanges,[80] rather they are usually used as a peer-to-peer payment method between illicit actors. However, there are many pure cryptocurrency exchanges which enable the conversion of these VCs to other VCs, thereby enabling cryptomarket vendors to deviously channel their proceeds into the fiat financial system. Thus, it is important to impose appropriate regulatory measures to hinder the flow of tainted VCs into the real economy.

4 Legal Regulation of Virtual Currencies

4A: International Initiatives

In various international fora, the rise of VCs has caused concern. In June 2019, the Financial Action Task Force (FATF), adopted an 'Interpretive Note to its Recommendation 15' (hereinafter IN) to respond to the increasing use of VCs for

[74] Jake Frankenfield, 'Darknet Market' (Investopedia, February 2018) <https://www.investopedia.com/terms/d/darknet-market-cryptomarket.asp> accessed 16 December 2019.
[75] *US v. Jones, Davis, and Nash*, (2013) <https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-three-individuals-virginia-ireland-and> accessed 16 December 2019.
[76] *US v. Sadler & White* (2013) <http://www.bellevuereporter.com/news/bellevue-couple-charged-with-silk-road-drug-sales/> accessed 16 December 2019.
[77] *US v. Faiella*, 39 F.Supp.3d 544 (S.D.N.Y. 2014).
[78] *US v. Force and Bridges* <https://www.courtlistener.com/docket/4181958/united-states-v-bridges/> accessed 16 December 2019.
[79] Details about these VCs accessible at https://coinmarketcap.com/.
[80] For example, in *Coinbase* none of these VCs are available.

money laundering and terrorist financing.[81] The amended recommendations require member countries to ensure that 'Virtual Asset Service Providers' (hereinafter VASPs) implement AML and KYC controls and be subject to effective monitoring and reporting obligations. On the same day, FATF also adopted a new guidance for a risk-based approach,[82] which includes a comprehensive recommendation-by-recommendation analysis for the implementation of the preventive measures in the context of VCs.

As stated by FATF, to qualify as a VASP an entity must both act as a business on behalf of customers and actively facilitate VC-related activities.[83] These activities include (i) exchange between VCs and fiat currencies, (ii) exchanges between one or more forms of VCs, (iii) transfer of VCs from one address or account to another, (iv) safekeeping or administration of VCs or instruments enabling control over VCs and (v) provision of services related to an issuer's offer of a VC.[84]

Almost every blockchain system participant is covered by this definition. Its ambit includes both virtual-to-fiat as well as virtual-to-virtual exchangers. Providers of kiosks, 'bitcoin ATMs' and VC brokerage services are also included in the above definition. Moreover, peer-to-peer or decentralised trading platforms may fall under the category of VASP where the platform facilitates the exchange, transfer, or other financial activity involving VCs.

In the context of wallet providers, only custodian wallet providers fall within the limits of part (iv) of the VC-related activities definition, as they safeguard the private key attached to an address.[85] Non-custodian wallet providers do not seem to provide a VC-related activity, because they do not usually have any control over the VCs. Finally, Issuers and other facilitators of ICOs are covered from the element (v). Notably, this definition promotes a 'technological neutrality' by determining whether a person engaged in VC-related activities is a VASP based on whether he is engaged as business or as an end-user, regardless of the technology deployed.[86]

---

[81] Press Release, FATF, 'Public Statement on Virtual Assets and Related Providers' (June 2019) <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html> accessed 16 December 2019.

[82] FATF, 'Virtual Assets and Virtual Service Providers: Guidance for a risk-based approach' (June 2019) 13 <https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> accessed 16 December 2019.

[83] Ibid 4.

[84] Ibid 13-14.

[85] FATF, 'Virtual Assets and Virtual Service Providers' (n 82) 16.

[86] The term technological neutrality is used here with the meaning that the same regulatory principles should apply regardless of the technology used. See Winston Maxwell and Marc

The FATF standards revolve around information sharing, KYC and CDD procedures as well as effective, proportionate and dissuasive sanctions.[87] A significant novelty introduced by the IN is that VASPs ought to be licensed or registered in the jurisdiction where they are created.[88] The IN acknowledges the money laundering and terrorist financing risks emerging from the global nature of VCs and it tables the broadest possible range of international cooperation.[89]

The same approach was adopted by the Bank of International Settlements (BIS) and the Financial Stability Board (FSB).[90] In particular, BIS suggested that FATF should foster the global implementation of its standards and 'focus on the point at which a cryptocurrency is exchanged into a sovereign currency' and 'on cryptocurrency infrastructure providers, such as crypto wallets.'[91]

4B: Developments in the EU

The inherent cross-border nature of VCs renders state-based legislative responses to VCs insufficient. An international Treaty for the regulation of VCs, apart from highly unlikely, would also be ineffective. This is because the time-consuming procedures that accompany an international Treaty render the latter unsuitable for regulating a fast-moving industry that orientates its innovation towards evading regulation. Considering that a solution is needed at a supranational level, this chapter analyses the applicability of EU legal frameworks on payment services, electronic money and AML to VCs. It is noted that the second Markets in Financial Instruments Directive (MiFID)[92] is not contemplated here since 'payment-type crypto assets are unlikely to qualify as financial instruments.'[93]

Bourreau 'Technology Neutrality in Internet, Telecoms and Data Protection Regulation' (2014) 1 Computer and Telecommunications Law Review 2.

[87] FATF, 'Virtual Assets and Virtual Service Providers' (n 82) 56.

[88] Interpretive Note (n 81) par. 3.

[89] Ibid par. 8.

[90] FSB, 'Crypto-asset markets: Potential channels for future financial stability implications' (October 2018), 15.

[91] Bank of International Settlements, 'BIS Annual economic report' (2018), 107

[92] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU [2014] OJ L 173/349.

[93] ESMA, 'Advice: Initial Coin Offerings and Crypto-Assets' (January 2019) 19. Similarly, given that the article focuses on the payments industry, the discussion regarding the applicability of general property law concepts to VCs is beyond the scope of this study. Cf. *AA v Persons Unknown* [2019] EWHC 3356 (Comm) according to which VCs are property within the meaning of English law.

Payment Services Directives

A key issue for the qualification of VCs in the EU regulation is whether they qualify as a 'fund' as per the payment services directives. That is because if a VC qualifies as a 'fund' under the second payment services directive (PSD2),[94] the provisions of the directive would apply to VC service providers, reducing significantly their suitability for financial crime abuse. According to article 4 par. 25 of the PSD2, the notion of funds is defined as 'banknotes and coins, scriptural money and electronic money'. This is yet problematic because we defined earlier VCs as 'tokens that can be used as a means of payment without having a legal tender status'. Hence, the PSD2 will not apply to classic decentralised VCs that do not qualify as e-money. A different approach suggested by the French banking supervisor (ACPR) arguing that VC exchanges are providing payment services since they receive 'banknotes and coins, scriptural money and electronic money' in exchange for VCs has gained only limited popularity.[95]

Overall, it appears to be a consensus that the PSD2 does not leave room to include VCs in the notion of 'funds'.[96] This is envisaged in the 5AMLD where it is stated that 'VCs should not be confused with the larger concept of funds as defined in point (25) of Article 4 of PSD2'.[97] Intriguingly, this choice has been made out of fear that should VC exchange platforms be subject to licensing and safeguarding requirements, this will further legitimise the use of VCs and create the unwarranted misconception to consumers that VCs are safe products.[98] This circular logic, however, is open to criticism on the basis that regulatory oversight usually urges regulated entities to greater transparency regarding their services and the associated risks.

E-money Directives

---

[94] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L 337/35 (hereinafter PSD2).

[95] Nikolaos Theodorakis, 'The Use of Cryptocurrencies for Illicit Activities and Relevant Legislative Initiatives' (2018) The Art of Crime 12 <https://theartofcrime.gr/the-use-of-cryptocurrencies-for-illicit-activities-and-relevant-legislative-initiatives> accessed 16 December 2019.

[96] Sergii Shcherbak, 'How Bitcoin Should be regulated?' (2014), 7(1) European Journal of Legal Studies 45, 61;

[97] 5AMLD, recital 10.

[98] European Banking Authority, 'Opinion of the EBA on the EU Commission's proposal to bring VC into the scope of Directive 2015/849' (2016) 4-5.

As elaborated above, VCs would only constitute regulated 'funds' if they qualify as e-money. The second e-money directive (EMD2) defines 'electronic money' as follows:[99]

> [E]lectronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in Article 4 of [PSD2], and which is accepted by a natural or legal person other than the electronic money issuer.[100]

According to this definition, classic decentralised VCs that operate in permission-less blockchains, such as *Bitcoin* or *Monero*, will not qualify as electronic money because they are not represented by a holder's claim on the issuer. It could be proposed that this definition applies to utility tokens, which incarnate a relationship between the token issuer and the token holder.[101] This view, however, neglects to consider that utility tokens are not usually accepted by a person other than the issuer. Even if these tokens are traded in the secondary market, they are still not accepted as a means of payment; rather they are traded for investment objectives.

This paper suggests that certain VCs could potentially qualify as e-money within the range of the EMDs.[102] Specifically, some VCs, such as stablecoins, may not only be accepted as a means of payment by other entities, but also represent a claim on the issuer.[103] For example, *Libra* will be represented by a claim against the *Libra* Association.[104] The latter will be the sole issuer of *Libra*, namely the only party able to create and destroy *Libra*.[105] Considering that *Libra's* business proposition 'is to enable a simple global currency'[106] and that, at the time of this writing, the consortium consists of many leading organisations, including Facebook, Spotify, Shopify, Uber, Lyft and

---

[99] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC [2009] OJ L 267/7.
[100] Article 2(2) EMD2.
[101] See, *supra* 1B.
[102] See *contra* Stefaan Loosveld, 'The 5th Anti-Money Laundering Directive: Virtual Currencies and Other Novelties' (2018) 33 Journal of International Banking Law and Regulation 297, 301.
[103] European Banking Authority, 'Report with advice for the European Commission on crypto-assets' (January 2019) 13.
[104] Cristian Catalini et al., 'The Libra Reserve', 2 <https://libra.org/en-US/about-currency-reserve/?noredirect=en-US#the_reserve> accessed 16 December 2019.
[105] See Libra Association (n 2) 8.
[106] Ibid 1.

Farfetch,[107] it is concluded that *Libra* will also be accepted by a legal person other than the issuer.[108]

In such cases, stablecoins should qualify as e-money and the issuer of such VCs may require an authorisation as an e-money institution.[109] As a consequence, these VCs would fall into the definition of 'funds' and the VC service providers may require additional licences as 'e-money institutions' under EMD2 and 'payment services providers' under the PSD2. Therefore, wallet providers and validating nodes would perform all the AML/CFT/CDD checks on users in the same way that current regulated digital banks and payment institutions do. As a result, the use of regulated VCs will not exacerbate the aforesaid financial crime risks as compared to fiat money.

Anti-Money Laundering Directives

The majority of VCs, however, do not fall within the scope of the e-money definition. They are unregulated and exploited for illicit activities, such as money laundering and illicit financing. In the EU law, the 4AMLD is the main regulatory response to these activities. It applies to 'obliged entities', such as financial institutions, estate agents, and other legal persons. Generally, it is accepted that VC system participants are not included in the notion of obliged entities under the (pre-amended) 4AMLD.[110]

By launching the 5AMLD, EU legislators aimed, for the first time ever, to target directly the financial crime risks emerging from the anonymity attached to VCs.[111] They espouse a 'balance and proportional approach' by empowering competent authorities to monitor the use of VCs through obliged entities.[112] The 5AMLD achieves this by introducing to the 4AMLD two new obliged entities: 'Providers engaged in exchanges between VCs and fiat currencies' and 'custodian wallet providers'.[113] Given that most users buy VCs through exchange platforms and use custodian wallet providers in their payments, they will now be required to verify their identity toward those intermediaries.

---

[107] Libra Association (n 2) 4.
[108] Dirk Zetzsche, Ross Buckley and Douglas Warner, (2019) 47 'Regulating Libra: The transformative potential of Facebook's Cryptocurrency and Possible Regulatory Responses' University of New South Wales Law LRS, 17-18.
[109] European Banking Authority, 'Report with advice for the European Commission on crypto-assets' (January 2019) 13.
[110] Niels Vandezande, *Virtual Currencies: A Legal Framework* (Cambridge Intersentia 2018), 298; 5AMLD, recital 8.
[111] 5AMLD recital 9.
[112] 5AMLD recital 8.
[113] 5AMLD Art. 1(1)(c)(g) and Art. 1(1)(c)(h).

The 5AMLD acknowledges, however, that these amendments will not adequately mitigate the anonymity risks attached to VC transactions, since users can also transact without such providers.[114] Therefore, it is envisaged that national Financial Intelligence Units (FIUs) should be able to gather information facilitating them to associate VC addresses to the identity of the owners.[115] In this regard, the 5AMLD leaves open the possibility of creating a central database with the details of all end-users.[116]

5 Critical Analysis of the EU regulatory framework

5A: The definition of Virtual Currencies in the EU

The 5AMLD clearly stipulates that to be considered as such, VCs 'must be accepted by natural or legal persons as a means of exchange'.[117] According to the taxonomy of VCs on the basis of their functionality, only 'exchange' or 'currency tokens' are intended to be used as a means of exchange, while 'utility' or 'investment' tokens provide different kind of rights to their holders. With the above in mind, investment and utility tokens do not fall within the perimeter of the 5AMLD.

This is problematic for two reasons. First, the wording of the definition in Art.1(2)(d) of the 5AMLD is conflicting with Recital 10 which suggests that 'the objective of this Directive is to cover all the potential uses of VCs' and not only their use as a medium of exchange.[118] Second, all kinds of tokens can be used for money laundering and terrorist financing. Besides, tokens that function as investment instruments can easily be traded for payment-type VCs in a secondary market.

Against this backgournd, it can be argued that national legislators would need to make explicit the application of the 5AMLD to VCs that are used for investment or store-of-value purposes.[119] At EU level, an altered definition should be adopted analogous to FATF's definition on virtual assets. The latter encompasses tokens that 'can be used

---

[114] 5AMLD recital 9.
[115] Thomas Frick, 'Virtual and Cryptocurrencies—Regulatory and Anti-Money Laundering Approaches in the EU and in Switzerland' (2019) 20 ERA Forum Journal of the Academy of European Law <https://link.springer.com/article/10.1007/s12027-019-00561-1> accessed 16 December 2019.
[116] 5AMLD Art. 65(1) *in fine*.
[117] See art.1(2)(d) of the 5AMLD, which inserts the VCs definition in the art.3(18) of the 4AMLD.
[118] 5AMLD, recital 10.
[119] Contrary, the application of the payment services directive and e-money directive is not indicated to this type of tokens.

for payment or investment purposes.'[120] Finally, the wording of the reformed definition should be open-ended in order to cover all possible type of tokens.[121]

5B: Assessing the Scope of the Regulation

By including virtual-to-fiat exchange services and custodian wallet providers under the scope of the AMLDs, the EU legislator attempted to mitigate the anonymity risks related to the use of VCs. This article suggests that the scope of the regulation is still inadequate, and it should be further broadened in order to ameliorate law enforcement's ability to trace transactions.

Virtual Currency Exchanges

Under the 5AMLD, all virtual-to-fiat currency exchanges qualify as obliged entities for AML/CFT purposes as long as they trade at least one VC within the definition of the 5AMLD against fiat currency.[122] As things stand, the Directive will only cover services that exchange 'currency' tokens against fiat currency and not providers engaged in exchange of 'utility' or 'investment' tokens against fiat currency.[123]

Furthermore, pure crypto exchanges (as set out in Chapter 1C) remain out of the 5AMLD's perimeter because they have no dealing with fiat currency. For example, a provider that offers a collection of well-known altcoins and accepts payments exclusively in *bitcoin*, if it does not qualify as a custodian wallet provider, is not covered by the 5AMLD.[124] Even though one could argue that virtual-to-virtual exchanges bear no direct relation with the fiat financial system, it is suggested herein that they can also be exploited from illicit actors to disguise the source of their VCs as well as be used to facilitate illicit transactions and means of payment.

This poses additional risks in the fast-moving world of VCs, as the network of actors that accept VCs as a means of payment can grow vastly. For instance, in New Zealand, paying salaries on VCs has been legalised.[125] Should VCs effectively become broadly accepted, the need to exchange VCs for fiat money through an exchanger might

---

[120] FATF, 'Virtual Assets and Virtual Service Providers' (n 82) 13.
[121] Haffke, Fromberger and Zimmermann (n 21) 14.
[122] Ibid.
[123] See *supra* Part 5A.
[124] Haffke, Fromberger and Zimmermann (n 21) 15.
[125] Daniel Palmer, 'New Zealand Tax Office Make it Legal to Pay Salaries in Crypto' (CoinDesk, August 2019) <https://www.coindesk.com/new-zealand-tax-office-makes-it-legal-to-pay-salaries-in-crypto> accessed 16 December 2019.

diminish over time. Consequently, virtual-to-virtual exchanges could be a focal point of control in monitoring money being transferred within VC networks.

In light of the above, member states should include pure cryptocurrency exchanges into the list of the obliged entities. Similarly, the EU legislator should overhaul its list of obliged entities pursuant to the FATF's notion of VASP, which ingeniously embraces exchange services between one or more forms of VCs.

Tumbler Services

Even though tumbler services are the entities that, for the most part, amplify the anonymity risks associated with the use of VCs, they are not included as obliged entities in the 5AMLD.[126] Given that tumbler services obscure the chain of transaction on one blockchain at a time, they could not qualify as VC exchangers either. Thus, it can be argued that the EU list of obliged entities should be amended to include not only virtual-to-virtual exchanges, but also exchanges within one form of VCs.

Wallet Providers

As stated above, custodian wallet providers have been incorporated in the list of obliged entities under 5AMLD, while non-custodian wallet providers have not been incorporated. The same approach is followed by FATF, since VASPs contain only services that have exclusive or independent control of the private key associated with an address.

It could be argued that wallet providers may elude regulation by requiring end-users to enter manually their private key. The question then becomes whether the scope of the 5AMLD should be extended to non-custodian wallet providers.[127] This will result, allegedly, in complete transparency of the virtual transactions and maybe in overregulation of VCs.[128] However, it is not always possible to extend the regulation to non-custodian wallet providers. For example, a hardware wallet provider does not provide a continuous service, but simply a product in which he is not supposed to have any oversight after the transfer.

On this point, the regulation seems to keep up with the current VC market developments, as most wallet providers are custodial. An additional step leading towards stricter regulation could be to further regulate the software non-custodian

[126] Haffke, Fromberger and Zimmermann (n 21) 18.
[127] Ibid 17.
[128] Ibid.

wallet providers, which provide end-users with software applications and interfaces that allow them both to access the network and save their keys locally. This will obstruct the above-mentioned potential loophole of the regulation.

Trading Platforms

Trading platforms that facilitate peer-to-peer transfer of VCs constitute a blind spot in the EU framework. Insofar they do not provide wallets to their users, trading platforms can function as unregulated online marketplaces where different VC holders can meet and interact directly. This has been acknowledged by FATF, which has incorporated entities that facilitate the transfer of VCs into the definition of VASP.[129]

It has been highlighted, however, that many trading platforms are 'decentralised', thus, it would be very hard to regulate them.[130] Even though the enforcement of the regulation might be complicated, law enforcement agencies should nevertheless have the appropriate legal infrastructure to do so, to the extent they can identify the owner or the operator of such platform . Consequently, trading platforms should be included in the list of obliged entities in the 5AMLD.

Issuers of Virtual Currencies

As stated above VC issuers could be divided in coin inventors and coin offerors.[131] It is evident that coin inventors are not obliged entities under 5AMLD. Contrary, coin offerors could be considered 'providers that engage in exchange services between VCs and fiat currencies' as long as they accept payment in fiat money.[132] Should pure crypto exchanges become obliged entities too, all coin offerors could fall within the scope of the 5AMLD.

The suggestion that the EU legislator unwittingly incorporated coin offerors to the definition of VC exchanges is arguably arbitrary. Specifically, the recitals of the 5AMLD do not mention coin offerors; if the legislator wanted to regulate the VC issuers, he would have simply done that explicitly. It could thus be argued that VC issuers should be regulated with more perspicuity in the Directive to avoid contradicting interpretations and fallacies. They could be included as a separable

[129] FATF, June 2019 (n 82), 16.
[130] IOSCO, 'Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms' (May 2019) 17 <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD627.pdf> accessed 16 December 2019.
[131] See *supra* Part 1C.
[132] Haffke, Fromberger and Zimmermann (n 21) 19.

obliged entity within the scope of the 5AMLD in the following form: 'providers engaged in services related to an initial offer of a VC'.[133]

5C: Regulating end-users: A proposal in Dispute

As highlighted above, regulation needs to be balanced between the attractiveness of VCs and the aforementioned financial crime risks. The EU legislator has taken, hitherto, a very soft approach towards unveiling the anonymity of end-users. Users that do not hold their VCs via a custodian wallet provider and do not transact through a regulated virtual exchange can still operate anonymously. The widening of the scope of the 5AMLD will impede only partially the enhanced anonymity risks, since users could still transact peer-to-peer without using any intermediary.

In this respect, it has been suggested by the EU legislator that it might become necessary to regulate end-users by registering their identities.[134] User's registration could take place either voluntarily or mandatorily.[135] A voluntary registration would, however, be ineffective since it would be absurd to trust a money launderer to willingly register his identity. In contrast, a mandatory registration would be very intrusive, and it might stifle the potential of VCs. Specifically, it would foist on end-users a regulatory burden that they would not have had they chosen to transact with fiat money. In addition to this, it would be impractical for national FIUs to maintain such central databases. Therefore, applying this regulation directly to end-users is not considered an appropriate and proportional legislative suggestion.

In legal theory it has been proposed to regulate end-users indirectly by holding them vicariously liable for interacting with undesirable VCs.[136] For example, users transacting with a permission-less blockchain-based VC which is well-known for being exploited by illicit actors are ultimately responsible for its value and maintenance. Hence, it might seem reasonable to hold these users vicariously liable for facilitating the unlawful activities stemming from the use of this VC by other users. Imposing such a risk to the end-users would function as a powerful deterrence for end-users to transact with high-risk VCs.[137] However, whether this would create causation problems is highly debatable from a fairness perspective, and it will undoubtedly impede the adoption of the lawful technology and stifle innovation.

---

[133] Derived from FATF June 2019 (n 82), 16.
[134] 5AMLD Art. 65(1) *in fine*.
[135] Houben and Snyers (n 4) 80.
[136] De Filippi and Wright (n 47) 176.
[137] Ibid.

5D: Introducing a comprehensive approach

For the purpose of pulling more end-users into the light, a more invasive approach towards anonymity is warranted. In this subsection, it is argued that VCs should be regulated according to their underlying technology.

Permissioned Blockchain-based VCs, such as *Libra*, *JPM coin* or *XRP Ripple*, should qualify as 'licenced VCs'. This would entail the EU financial services law applying to these VCs. As stated above, some of these VCs fulfil the requirements of the definition of e-money.[138] This article suggests that the e-money definition should be revised in order to explicitly include all VCs that operate in a permissioned blockchain payment system. Consequently, issuers of such VCs would require authorisation as e-money institutions. Accordingly, entities which undertake blockchain payment services, such as the execution of payments or money remittance, would fall within the perimeter of the PSD2[139] and they would require appropriate licencing. Hence, the licenced blockchain system participants would perform all the AML/CFT/KYC obligations in the same way as the fiat payment services providers. This will comprehensively thwart all the identified financial crime risks since regulated intermediaries will provide monitoring on the transactions, thereby rendering VCs unattractive for illicit behavior.

Permission-less blockchain-based VCs, such as *Bitcoin*, *Ether* or *Monero*, should qualify as 'unlicenced VCs'. This implies that the EU financial services law shall not apply to these VCs. The absence of known issuers and central administrators renders the regulation of permission-less blockchain VCs through obliged entities as the only viable solution. The widening of the perimeter of the 5AMLD, by expanding the list of obliged entities, will undoubtedly bring more users' identities into light. On the other hand, illicit actors and so-called 'cypherpunks' are increasingly developing new decentralised methods that improve the privacy of transactions. For example, Mathew Green, a John Hopkins University professor, has designed *Zerocoin*, an extension to *Bitcoin* that provides end-users with complete anonymity without being a tumbler service.[140] It is expected that without a comprehensive regulatory framework, code developers will constantly be a step ahead of regulation.

This article suggests that a comprehensive solution which would tackle the anonymity associated with permission-less blockchain-based VCs is two-fold. First, apart from

---

[138] See *supra* Part 4B.

[139] Payment services are listed exhaustively in Annex I of the PSD2.

[140] Ian Miers, 'Zerocoin Project' (*Zerocoin.org*, 2020) <http://zerocoin.org/> accessed 20 October 2020. Zerocoin has now been succeeded by the Zerocash protocol and its native VC, *Zcash.*

accepting the alterations proposed in Chapter 5B, all VC service providers should also be licenced in such a way that they would be accountable to the authorities. Second, and most important, it should be made mandatory for users to transact only through a licenced intermediary. For example, end-users would only hold and trade VCs lawfully if they do so through a licenced custodian wallet provider. This will allow the supervisory authorities to attach regulation to an identifiable third person. The latter entity could also be held accountable for remedying victims of fraud and other aggrieved users. The regulatory burden will not be imposed to end-users but to businesses, thence the attractiveness of VCs will not be stifled. These provisions could be either inserted as special provisions to the current AMLDs or form part of a framework exclusively for VCs.

A probable counterargument against our regulatory proposal for permission-less blockchain VCs would be that part of the Blockchain's innovative potential is that has cut out such 'middlemen.' The same contention regarding the removal of all middlemen was repeatedly being made when the Internet first pushed into mainstream consciousness.[141] Nonetheless, despite the fact that the Internet eliminated the need for some middlemen, as it gained broad adoption it enabled the development of new intermediaries to which regulation could be attached.[142] A similar pattern is unfolding in the course of blockchain-based systems. It is argued that imposing just one quasi-mandatory intermediary would not restrict the revolutionising potential of permission-less blockchain payment systems since the latter still cut-off a whole chain of banking intermediaries.

Lastly, meta-regulation should not be overlooked. The latter suggests that regulators may seek to induce the regulated entities to develop their own, internal, self-regulatory responses to public problems.[143] In our context, the proposed regulatory imposition will prompt the entities engaging in VC activity to co-regulate themselves and accept in the course of their business only VCs stemming from lawful wallets.[144] Illicit users operating without a licenced intermediary would not be able to transact with lawful users. Consequently, the expected utility from engaging in VC related

---

[141] Andrew L Shapiro, 'Digital Middleman and the Architecture of Electronic Commerce' (1998) 24 Ohio Northern University Law Review 795.
[142] De Filippi and Wright (n 47) 179.
[143] Cary Coglianese and Evan Mendelson, *The Oxford Handbook of Regulation* (Oxford University Press 2010), 150.
[144] The term co-regulation is preferred by some legal scholars; see Michele Finck, *Blockchain Regulation and Governance in Europe* (Cambridge University Press 2019) 172 who argues that a model of polycentric co-regulation would be a suitable approach for regulating decentralised blockchain ecosystems.

criminal behaviour will be reduced significantly and the financial crime risks will be mitigated in a virtual ecosystem which would be clearly delineated.

Conclusion

VCs present a challenge for legislators around the globe. On the one hand, they have the power to enhance or even supplant the traditional payment systems. They could offer a number of potential benefits, and regulators should be careful not to hinder these innovations. On the other hand, VCs create new financial crime risks. Using the classic utility model of criminal behavior as a lynchpin, this inquiry identified the risks raised by the anonymity, decentralisation and cross-border nature of VCs in the context of money laundering, terrorist financing and illicit flow of money.

The first objective of this article was to analyse the extent at which VCs are regulated under the current EU regulatory framework on e-money, payment services and AML. The main conclusion to be drawn with regard to this issue is that *de lege lata* only the AML regime undoubtedly applies to VCs. Contrary, the applicability of the EMD2 and PSD2 to VCs is open to interpretation and should be examined on a case-by-case basis.

Accordingly, the article probed how regulation needs to be reorientated in order to balance between the attractiveness of VCs and the financial crime risks associated therewith. On this matter, the paper attempted to introduce a comprehensive solution based on the underlying technology of VCs. With regards to permissioned blockchain-based VCs, the article proposed that the EMD2 and PSD2 are in need of modification to explicitly integrate these VCs under their ambit. In respect of VCs that operate in permission-less blockchains, it is firmly suggested to impose a compulsory intermediary between the end-user and the blockchain.