CHALLENGES THAT CRYPTOASSET ANONYMITY CREATES FOR TAX ADMINISTRATION

Sergio Avalos
International and European Tax Law, Maastricht University, Netherlands.

ABSTRACT

The virtual currency market has grown significantly worldwide in the last decade. Innovations have made it necessary for the concept of cryptocurrencies to be broadened to include so-called "cryptoassets". Countries differ in their legal frameworks for the taxation of cryptoassets and in how they address the challenges that cryptoassets create for tax administration. The pseudonymity of cryptoassets presents the biggest challenge when tax administrations are attempting to properly enforce tax compliance and counter tax evasion. This article provides an overview of the existing legislation addressing the pseudonymity of cryptoassets with an emphasis on the European Union (EU)'s Anti-Money Laundering Directive 5 (AMLD5) and the United States' Foreign Account Tax Compliance Act (FATCA). It argues that both legislations have limitations in respect of their coverage of all stakeholders involved in the cryptoasset market, and provides insights into recent public consultations by the Organisation for Economic Development (OECD) and proposed legislation by the EU on the matter. Finally, it raises the question of whether or not a coordinated effort at the global level would be the best approach to take in order to address a problem that is common across tax administrations around the world: the pseudonymity of cryptoassets.

Keywords: *Cryptoassets, Cryptocurrencies, Anonymity, Tax Administration, AMLD5, FATCA.*

INTRODUCTION

The Problem

Since the invention of the first cryptocurrency, Bitcoin (BTC) in 2008, the virtual currency market has expanded worldwide. More than 10,000 cryptocurrencies exist today, with Ethereum (ETH), Ripple (XRP), Tether (USDT), BNB (BNB), and Solana (SOL) being among the best known.[2] There has been massive growth in the adoption of distributed ledger technologies in recent years and, naturally, new inventions and innovations have become a reality. The scope of the market is much wider than it was and includes so-called "cryptoassets". There are multiple definitions of the term "cryptoasset", with the European Central Bank (ECB), the International Organization of Securities Commissions (IOSCO), the Financial Stability Board (FSB), the European Securities and Markets Authority (ESMA), and the European Banking Authority (EBA) each having its own definition (Houben & Snyers, 2020). However, in general, use of the term allows cryptocurrencies and so-called "tokens" to fall within a common category.

In recent years, the number of cryptoasset transactions taking place in the world has increased dramatically. Cryptoassets are now used both as a means of payment and a means of investment. Their use as a means of investment is of particular public interest as this has resulted in the generation of large profits for their owners.

One of the problems that can be observed at country level is the fact that the cryptoasset market is only regulated to a limited extent and, in many cases, does not have a specific legal or regulatory recognition. In the case of cryptocurrencies, this

happens because they are not a legal tender or equivalent, and are not considered to be foreign currencies as they do not have a specific central and territorial issuer that supports them. In most cases, local central banks do not support cryptocurrencies and have no power to regulate them.

Cryptoassets are based on cryptographic technologies that allow their issuance, validation, and registration in a decentralised manner. Although cryptocurrencies are not legal tender and do not have intrinsic value, they have begun to be used for commercial exchanges. Consequently, the acquisition, sale, use, or possession of cryptoassets is of undeniable tax significance. One of the main difficulties faced by the tax administration is the relative anonymity that cryptoassets such as Bitcoin offer to their users. This is because blockchain technology allows the user to hide their real identity behind a pseudonym, thanks to the double key system (consisting of a public and a private key) on which it is based. The anonymity provided by cryptoassets presents an important challenge for the tax administration, which must adapt the schemes and resources that it has traditionally used so that it can use them in its new fight against concealment and tax fraud. The concealment and fraud take place in an area beyond its control—that is, on a peer to peer (P2P) network of private users whose identity is unknown, and where there is no intervention by a centralised authority (such as the banking system, for example) which would be able to provide information to the tax administration.

There is a lack of doctrinal opinion or extended judicial or administrative jurisprudence that discusses or clarifies these points. There is also no specific regulatory framework in each country that allows for the specification and classification of the operations and activities carried out with cryptoassets within the current tax legislation. The lack of consensus when dealing with the anonymity behind cryptoassets has generated discussion, caused controversy, and raised a number of questions for both tax administrations and those investing in this type of digital and virtual asset.

There is currently no consensus at the country level about how to solve the problem generated by anonymity in cryptoassets when attempting to determine and control taxes, although the most important problem to solve if tax evasion is to be minimised.

From a technological perspective, this anonymity prevents cryptoasset transactions and operations from being properly monitored. The traditional system used by tax administrations to obtain information, which ensures tax compliance by taxpayers, is based on a centralised structure of intermediaries. These are banks, employers, and various institutions that are obliged to obtain information from taxpayers and transmit it to the tax authority, so that the tax authority has sufficient information to demand compliance and impose fines, add interest, or even initiate legal action if the taxpayer does not voluntarily comply with their tax obligations within the relevant term. The emergence of cryptoassets disrupts this scheme.

The anonymity provided by cryptoassets to their users makes it difficult, if not impossible, for tax administrations to be able to ascertain their true ownership. This undermines the current protocols for obtaining information and leaves tax administrations without their most effective tool for ensuring tax compliance, whether that compliance is voluntary or coercive.

The research question that this article will try to answer is the following: What challenges does cryptoasset anonymity create for tax administrations?

From an anonymity perspective, the challenges presented at the cryptoasset level are the same as those presented at the cryptocurrency level (the most popular cryptoassets), which allows us to focus this article from a cryptocurrency perspective and, at the same time, to extrapolate the conclusions to cryptoassets.

The author aims to contribute to the literature by providing a detailed investigation and analysis of the problems that cryptoasset anonymity generates from a tax administration perspective. Anonymity is the major issue related to the cryptoassets market when it comes to tax evasion. If a tax authority cannot access information about the parties involved in a cryptoasset transaction because of the pseudonymity of those parties, it cannot take action over any tax compliance breach or tax evasion that occurs. This could create a tax gap.

The research question will be addressed by analysing: the main concepts behind blockchain technologies; the different treatments that countries give to cryptocurrencies within their regulatory approaches; the theoretical framework, definition, and origin of cryptoassets; cryptoassets' characteristics and uses; the types of cryptocurrency available; who the participants in the cryptocurrency market are; the regulations in force in the European Union and in the United States regarding the anonymity behind cryptocurrencies; the difficulties that anonymity in cryptocurrencies generates from a tax perspective; current public consultations, and potentially forthcoming legislation and guidance from the European Union and the OECD with regard to the matter; and topics that could be interesting to investigate in any future research conducted in order to enrich the debate from a public policy perspective so as to solve an important problem—how to fight tax evasion involving the use of cryptoassets.

This article begins with a discussion about prior research into cryptoassets and taxation, with a focus on cryptocurrencies. This is followed by a detailed explanation of the theoretical framework and environment of blockchain, cryptoassets, and cryptocurrencies (section 2). Section 3 clarifies the actual regulatory and taxation approaches that some countries have adopted, and discusses the approaches that the European Union and the United States have taken in respect of cryptocurrencies and their anonymity. In addition, section 3 provides an overview of recent and proposed public consultations and legislation, such as the EU's Directive on Administrative Cooperation 8 (DAC8) and 6th Anti-Money Laundering Directive (AMLD6), and the OECD's Cryptoasset Reporting Framework and Amendments to the Common Reporting Standard. Section 4 broadens the discussion and considers which topics could be interesting to investigate in future research in order to enrich the debate from a public policy perspective. Finally, section 5 provides some conclusions.

Prior Research into the Taxation of Cryptoassets

Prior research into the taxation of cryptoassets has focussed primarily on the nature of cryptocurrencies from legal and financial perspectives, and on whether or not they should be considered to be fiat money or financial assets for regulatory purposes. A great deal of attention has been paid to the tax consequences that these different approaches may have. To date, the vast majority of studies have investigated Bitcoin and its treatment by various countries in respect of its character either as property, or as private money or foreign currency, and/or the tax consequences of conducting transactions with cryptocurrencies, and how to determine the tax costs and value of cryptocurrencies at the time that they are

alienated, sold, or exchanged in order to determine whether there was a capital gain of a greater value.

Bal (2013), for example, examines the phenomenon of virtual money, looking at the tax consequences arising from its use and distinguishing it from electronic currency. The study discusses two prominent virtual currency schemes: Bitcoin and virtual world money. The author outlines the most common income tax problems faced by virtual currency users and regulators in order to present the tax implications of conducting virtual currency exchanges. The main research question is whether or not virtual currency constitutes taxable income (Bal,2013).

The same author details Bitcoin's main characteristics and discusses "whether Bitcoin should be regarded as money in the economic and legal sense, and whether income in the form of virtual currency should be subject to tax" (Bal, 2014a, p. 1). The study reflects on whether or not it would be a "right and good policy" to tax virtual income (Bal, 2014a, p. 1). The author bases their analysis on "the main four axioms upon which a tax system ought to be based" as detailed "by Adam Smith in *The Wealth of Nations*", i.e. "equity, certainty, convenience and efficiency" (Bal, 2014a, p. 9). They state that there is a strong case against taxing virtual income because of "illiquidity, valuation and compliance difficulties" (Bal, 2014a, p. 15). One of the key reasons why the author arrives at this conclusion is that, in the case of Bitcoin, the "online marketplace is an anonymous marketplace where individuals can easily conceal their identities and locations" and, as a result, "tracking virtual income of taxpayers is well beyond the capacity of tax authorities" (Bal, 2014, p. 15). Bal (2014a) states that, in this case, "voluntary compliance is not a workable solution since taxpayers have little incentive to report something that is not likely to be detected" (p. 15). The author concludes, therefore, that "the general principles of taxation imply that virtual income should remain tax free" (Bal, 2014a, p. 15).

Bal (2015) examines "the treatment of Bitcoin for [Value-Added Tax] VAT and financial reporting purposes" from a regulatory perspective, particularly in relation to the European Union (p. 1). The main research questions posed in the study were "whether exchanges of bitcoins constitute taxable supplies under the VAT Directive (2006/112) [footnote excluded] and, if so, whether a VAT exemption may be applied" (Bal, 2015, p. 1). The author concludes that the "tax authorities of different countries have diverging views on whether bitcoin transactions are subject to VAT" (Bal, 2015, p. 10) and that, "in many EU Member States, such transactions have been declared exempt" (Bal, 2015, p. 3).

Bal (2019) provides an overview of virtual currency regulations at that time in Australia, Germany, the Netherlands, the United Kingdom, and the United States, and proposes "a methodology for creating an effective regulatory framework for the taxation of virtual currencies" (p. 219). This methodology consists of four steps: (i) conducting "a data driven assessment" which includes investigating the concept of virtual currencies, their definitions, and their usage in order to regulate them (Bal, 2019, p. 225); (ii) selecting a "method of regulation"—the author highlights the differences between approaching this by means of legislation and by supplementing legislation with more detailed administrative guidelines (Bal, 2019. p. 225); (iii) ensuring that the regulatory framework is sound from an informational and communicational perspective—tax administrations should "provide comprehensive guidance to help taxpayers comply with their tax obligations resulting from the use of virtual currency" (Bal, 2019, p. 228); and (iv) ensuring that a sound approach to

monitoring and governance is taken—the author briefly highlights the threat that anonymity generates for tax compliance, recommends that the compliance effort is focussed on a small number of exchange service operators and wallet providers, and suggests that these efforts should be aligned with the Anti- Money Laundering Directives.

A recent study conducted by the OECD (2020) provides an overview of the approaches taken to cryptoasset taxation (in the form of income tax, value added tax [VAT], and property taxes) by multiple countries. The report states that "G20 Leaders and Finance Ministers have asked international organizations to analyse the risks created by crypto-assets", since they are "in rapid development and tax policymakers are still at an early stage in considering their implications" (OECD, 2020, p. 3).

As previously discussed, most of the previous research into cryptocurrencies has been based on analyses of Bitcoin and its tax qualification. This article focusses on a broader concept by analysing cryptoassets and the tax administration issues related to the anonymity that surrounds them.

THEORETICAL FRAMEWORK OF BLOCKCHAIN AND CRYPTOASSETS

What is Blockchain?

Blockchain is the technology behind the large variety of cryptoassets currently in circulation. It is a distributed, decentralised, secure database in which transaction blocks are signed with digital signatures using private keys, and functions as a large ledger of accounts in which each entry is called a block (Bal, 2014a; Hellani et al., 2018). It becomes a chain because each new block is linked and encrypted with the previous block to ensure that transactions are private and secure (Natarajan et al., 2017). Each block has a timestamp which details the day and time that the record was created and which cannot be modified retroactively. There must be several users within the chain who are responsible for verifying those transactions in order to validate them and so that the block corresponding to each transaction is recorded in that large ledger of accounts (Houben & Snyers, 2018).

Contrary to popular belief, blockchain technology does not need to be private and anonymous. In the specific case of cryptocurrencies, this was the design that was implemented, but blockchain applications without anonymity, and where all information is public, can exist.

The Definition and Origin of Cryptoassets

According to a study conducted by the European Parliament, a cryptoasset is a digital asset that:

> *Is recorded on some form of a digital distributed ledger secured with cryptography,*
> *Is neither issued nor guaranteed by a central bank or public authority, and*
> *Can be used as a means of exchange and/or for investment purposes and/or to access a good or service [footnote removed]. (Houben & Snyers, 2020, p.17).*

In general, scholars exploring cryptoassets differentiate between cryptocurrencies and tokens. A cryptocurrency is a virtual or digital currency which, unlike fiat money, is not in a physical form (such as paper or metal) but which still has the characteristics of a currency, such as being a means of exchange, a unit of account, or a store of value (Bal, 2014a). Cryptocurrency's origins begin with Satoshi Nakamoto, a pseudonym for one or more still unidentified people, who proposed a new electronic money system—Bitcoin—that would allow direct payments to be made between users without the intermediation of a financial institution (Nakamoto,

2008). No traditional regulatory body issues, administers, or guarantees a cryptocurrency so these functions are only fulfilled by the mutual agreement of the cryptocurrency's user community. A completely decentralised system is utilised for transfers between users, with no intermediaries involved, and the generation and use of the cryptocurrency is based on cryptographic principles so as to guarantee the safety and protection of the operations (Grinberg, 2011).

Tokens, on the other hand, are cryptoassets that "offer their holders certain economic and/or governance and/or utility/consumption rights [footnote removed]" (Houben & Snyers, 2020, p.18). They are digital representations of rights or interests to products, services, or assets (ESMA, 2019), and it is common to see the issue of tokens to raise funds for different projects or start-ups (Annunziata, 2020). There are subcategories of token, such as utility tokens, security tokens, and non-fungible tokens (NFTs) which, for the purposes of this article, all share the same properties from an anonymity perspective.

Why Do People Use Cryptoassets?

Among the questions that have been asked by regulators worldwide is why users choose to utilise cryptoassets instead of traditional currencies or securities. Are cryptoassets better payment or investment alternatives than other currencies or securities? What advantages do cryptocurrencies offer in terms of their transaction and payment systems that are not provided by traditional markets? What advantages do cryptoassets have in terms of investment that cannot be found in the financial market for stocks, bonds, or other asset classes?

There is a great variety of cryptoassets. Although some are similar to each other, there are some variations in terms of the way in which they are structured, the technology used for their operation, and the degree of anonymity involved.

Cryptoassets can be compared using a number of parameters: their decentralised nature; whether they run on permissioned or permissionless technology; whether or not they were initially offered by an identifiable person or entity; whether or not they are electronically traded; whether or not they can be directly converted into fiat money; whether or not they can be used as a medium of exchange; and whether they are anonymous or pseudonymous (Houben & Snyers, 2018). Four common properties that have probably been key to the success of a large number of cryptoassets are: pseudonymity, decentralisation, the ability to be electronically traded, and the ability to be directly convertible into fiat money (Houben & Snyers, 2018).

Among the arguments regarding the attractiveness of cryptocurrencies is the fact that they allow transactions and payments to be made instantly, even when these are being made between people or companies located in different countries. In the international banking system, it can take several days for a Society for Worldwide Interbank Financial Telecommunications (SWIFT) transfer—an international transfer between financial institutions—to be made. Local currencies also need to be converted into dollars or other primary currencies and the recipient must then convert the amount transferred into their preferred currency. Fees are charged both in respect of the SWIFT transfer and the currency exchanges. Cryptocurrency transactions can be fast and cheap alternatives, with both buyers and sellers benefiting because the transactions do not incur bank or credit card fees. On the other hand, cryptocurrencies are not subject to the monetary policy of any central bank, so their price is always determined by the market in terms of supply and demand.

Concerns have been raised by the main central banks about the risks that could arise within the financial system as a result of, for example, the volatility and illiquidity of cryptocurrencies (ECB, 2015). Cryptocurrencies can also be used as investment mechanisms and converted into fiat money or other cryptocurrencies at a value that constantly varies in the cryptocurrency market according to the rules of supply and demand. In addition, when buying and selling cryptocurrencies, once a transaction has been executed and validated, it cannot be reversed, therefore providing a full collection guarantee.

From an investment point of view, cryptoassets are in a different asset class from the traditional assets, such as stocks, fixed income assets, commodities, and real estate, which, in theory, could be used to diversify an investment portfolio.

A relevant factor to consider is that there is no clear regulatory framework at country level regarding the treatment or nature of cryptoassets. In some countries, they are considered to be a currency like any other, while in others, they are considered to be assets. There is no unanimity in the criteria as to whether their increase in value generates capital gains or not, which leads to the creation of various opportunities that are not present in other asset classes in terms of generating tax-free profits (Cumming et al., 2019). Another characteristic that makes cryptocurrencies attractive is their anonymity, whereby even if the profits derived from them were taxable, it is, in practice, almost impossible to determine who was behind the transactions and, therefore, to detect tax evasion or tax fraud.

Blockchain technology, in the case of cryptocurrencies, was designed to be anonymous. For what purpose is a question that remains open. What is clear is that while this has benefits, it also presents dangers which are of great concern for the authorities, not only at the tax level, but also in relation to money laundering and the financing of terrorism.

The Issue of Anonymity

It is generally interpreted that cryptocurrencies use systems that guarantee the anonymity of their users due to two characteristics: first, internally, cryptocurrencies are not necessarily related to real identities, and second, from a cryptographic perspective, the keys used to make transfers do not contain the users' real identities.

According to a report by the Financial Action Task Force [FATF], "cryptocurrency relies on public and private keys to transfer value from one person [individual or entity] to another, and must be cryptographically signed each time it is transferred" (FATF, 2014, p. 5). Each of these transfers is registered in a blockchain, and prepared and distributed among peers via a decentralised system. The organisation notes that "the safety, integrity and balance of cryptocurrency ledgers is ensured by a network of mutually distrustful parties (in Bitcoin, referred to as miners) who protect the network in exchange for the opportunity to obtain a randomly distributed fee" (FATF, 2014, p. 5).

The cryptographic systems used in cryptocurrencies can broadly be classified as symmetric and asymmetric. When a symmetric or private key encryption system is used, both the sender and the receiver of a message must use the same key to encrypt and decrypt that message respectively. On the other hand, when an asymmetric key system is used, only one key (the public key) is distributed, eliminating the problem of transmitting a secret key between sender and receiver.

The public key can be utilised by any user who wishes to communicate with its owner and the private key can be used exclusively by its owner to decipher and sign messages.

The use of asymmetric key cryptography or an anonymous public key system ensures anonymity because although each node in the system has access to the blockchain, it only contains information about the amount involved in and the timing of the operation, together with the participants' public keys. It does not contain any additional information of a personal nature. Therefore, the anonymity in the system lies in the impossibility of linking any public key with its user. The identity of the person involved in the operation could only be known if a particular subject is somehow identified by way of an address or public key. In this case, it would be easy to track all the operations that had been performed by this subject within the blockchain.

On the internet, anonymity can be understood in two different ways: in a literal way (i.e. acting without any name or identity), or in a relative way (i.e. operating by means of a pseudonym or false name). In the case of cryptocurrencies, users publicise a public key or address. Their real identity is not known and they use a pseudonym (i.e. anonymity is relative rather than absolute). This is what is commonly referred to as pseudonymity and does not, per se, ensure the anonymity of the users. In some cases, it is possible to establish a relationship between the public key or address of the cryptocurrency and the real identity of the user. However, anonymity can be achieved if the system has an operative unlinkability property, something that is achievable thanks to blockchain technology (Koshy et al., 2014; Ober et al., 2013; Reid & Harrigan, 2013). The term "unlinkability" refers to the idea that any user who accesses the information contained in the blockchain will find it impossible to obtain more information than is contained in those records. It is also worth mentioning that, in addition to the intrinsic anonymity enabled by blockchain technology in respect of cryptocurrencies, there are tools that exist that allow users to intentionally eliminate the traceability of their cryptocurrency operations. Some examples of this are the use of several accounts by the same user (each with a different public key), the use of software or services known as mixers or tumblers that mix cryptocurrencies from multiple addresses in order to make it difficult or impossible to track the user who performed the operation, or the exchange of one cryptocurrency for another cryptocurrency (Herrera-Joancomartí, 2014).

In the case of cryptocurrencies, due to the decentralised nature of blockchain technology and the relative anonymity provided by the system, it is not possible to know the true identity of the user behind the public key. However, since all operations are collected in the blockchain openly, the tax administration could, by using appropriate software, track all operations carried out by a specific account by identifying it via its public key. As a result, the tax authority could ascertain the account's cryptocurrency balance and a record of all transactions that have been made to or originated from that account, but without knowing who owns it.

Participants in the Cryptoasset Market

The players involved in the cryptoasset market include cryptoasset users, miners, cryptocurrency exchanges, wallet providers, trading platforms, coin inventors, token inventors, coin offerors, and token offerors (ECB, 2015).

According to the FATF (2014), a user is a person/entity who obtains virtual currency and uses it to purchase real or virtual goods or services (or send transfers

in a personal capacity to another person (for personal use), or who holds the virtual currency as a (personal)investment. (p. 7).

The FATF (2014) notes that there are several ways in which cryptocurrencies can be obtained. Users can buy cryptocurrencies using fiat money via an exchange or directly from another user, receive them as payments in exchange for, for example, goods or services, or generate them through a process called coin mining (FATF, 2014).

A miner is someone who validates blockchain transactions by solving cryptographic puzzles. The process of mining relates to cryptocurrencies that are based on a consensus mechanism known as Proof of Work (PoW). The miners maintain the cryptocurrency network and keep the registry up to date and secure. They can work in isolation or establish unions in order to achieve a much greater computing power. The work that they perform is of high complexity and, at the same time, incurs a high cost because of the energy used, so they receive compensation in the form of cryptocurrencies.

Cryptocurrency exchanges provide users with cryptocurrencies in exchange for fiat money, funds, or other forms of cryptocurrency in exchange for a fee or commission (FATF, 2014). The FATF (2014) notes that exchanges "generally accept a wide range of payments, including cash, wires, credit cards and other virtual currencies" (p. 7). The FATF (2014) adds that they can function in the same way as a stock exchange or exchange office, and that users often utilise exchanges "to deposit and withdraw money from cryptocurrency accounts" (p. 7). Many cryptocurrency exchanges also "act as wallet providers" (ECB, 2015, p. 8).

Wallet providers furnish cryptocurrency users with digital wallets "which are used for holding, storing, and transferring coins" (Houben & Snyers, 2018, p. 27). A wallet provider will usually convert a "user's transaction history into an easily readable format, which looks much like a regular bank account" (Houben & Snyers, 2018, p. 27).

Trading platforms differ from cryptocurrency exchanges in two aspects. First, "they do not buy or sell coins themselves" (Houben & Snyers, 2018, p. 27). Second, "they are not run by an entity or company that oversees and processes all trades, but they are operated exclusively by software (i.e. there is no central point of authority)" (Houben & Snyers, 2018, p. 27).

Coin inventors develop "the technical foundations of a cryptocurrency and set the initial rules for its use" (Houben & Snyers, 2018, p. 28). The identities of some coin inventors are known but this is not always the case (ECB, 2015). Coin offerors are "individuals or organisations that offer coins to cryptocurrency users upon the coin's initial release, either against payment (i.e. through a crowdsale) or at no charge (i.e. in the framework of a specific (sign-up) program…)" (Houben & Snyers, 2018, p. 28; see also OECD, 2018; Spagnuolo et al. 2014). The terms inventors and offerors can also be applied in respect of tokens.

CRYPTOASSET REGULATION AND TAXATION

Cryptoasset Regulatory Framework

When it comes to cryptoassets, it is important to highlight that existing legislation is restricted to cryptocurrencies and does not cover the broader category of cryptoassets, which includes tokens. This limits the regulatory analysis in this article to cryptocurrencies.

Since the use of cryptocurrencies began to increase, their regulation has been

debated around the world. Regulators from across the globe are looking at whether and how to regulate cryptocurrencies, and there is currently no consensus about how to do it. The rise of cryptocurrencies has created interesting tax issues. The two most visible and controversial of these are whether cryptocurrencies should be considered to be currencies or standard propertyfor tax purposes, and how their cost and value must be calculated when determining a capital gain. Their taxation as property makes their everyday use impractical because every transaction forces the taxpayer to recognise gains and losses. On the other hand, calculating the cost of a cryptocurrency is a complex task in the case of a mining process, because the cost related to the energy used by a computer when solving cryptographic puzzles has to be considered as part of the total costs for tax purposes. Countries are taking a decentralised approach to cryptocurrency regulation; they treat cryptocurrencies differently. In the case of the United States, the Internal Revenue Service (IRS) views cryptocurrencies as property that is similar innature to traditional assets, while China does not recognise cryptocurrencies and has banned their trading as well as Initial Coin Offering (ICO) issuance (Cumming et al., 2019). India does not consider cryptocurrencies to be legal tender and considers growth in capital from them to be capital gains (Cumming et al., 2019).

Countries within Europe also have different views on how cryptocurrencies should be treated. A Langer (2017) note that the United Kingdom takes a case-by-case approach to cryptocurrencies and treats them as either assets or private money. Germany considers cryptocurrencies to be private money and their sale does not incur capital gains tax, but cryptocurrency investments are subject to income tax if they are held for less than a year (Langer, 2017). In Switzerland, cryptocurrency sales are not subject to capital gains tax, but residents' cryptocurrency holdings are subject to income tax, profit tax, and wealth tax (Langer, 2017).

Undoubtedly, the previous questions regarding the treatment of cryptocurrencies are relevant as they could create mismatches and tax planning challenges, but they are not the most crucial problems to solve from a tax perspective. The most important topic related to cryptocurrency that needs to be addressed is anonymity. According to Houben and Snyers (2018), "anonymity prevents cryptocurrency transactions from being adequately monitored, allowing shady transactions to occur outside of the regulatory perimeter" and "is also the major issue when it comes to tax evasion" (p. 51). They state that "when a tax authority does not know who enters into the taxable transaction, because of the anonymity involved, it cannot detect nor sanction this tax evasion" (Houben & Snyers, 2018, p. 53). The United States, via the Foreign Account Tax Compliance Act (FATCA), and the European Union, via the Anti-Money Laundering Directive 5 (AMLD5), are leading the fight against cryptocurrency anonymity by taking different approaches.

Cryptocurrency Anonymity

Although the tax authority may have access to the information that is stored on the blockchain, it is still necessary to be able to somehow link the user's account (public key) with their real identity to ensure that they comply with their tax obligations. The tax authority could take various approaches in order to collect the necessary information. It may attempt to obtain this information on its own, may consult other tax authorities based on the increasing exchange of information within

the tax authorities, or may wait for the taxpayer involved to provide such information. To identify the holders of cryptocurrency accounts, tax authorities can resort to complex methods based on techniques for the deanonymisation of cryptocurrency users by grouping cryptocurrency addresses controlled by the same user together, attempting to determine patterns of behaviour, and eventually using models to determine their identity. Another key challenge that tax authorities' face in the fight against cryptocurrency-related tax evasion is that there is often no central intermediary, such as an issuer, who would normally be the target of regulation. Therefore, in such cases, the question of which cryptocurrency market players regulation should be attached to is an important one. The relative anonymity offered by cryptocurrencies is easy to maintain as long as the user does not leave the system but is no longer guaranteed when the user leaves it (for example, by converting the cryptocurrencies into legal tender). A possible action to consider in response is to broaden the concept of a financial intermediary to include exchangers within the cryptocurrency market.

The legislative approach taken by the European Union and the United States requires users to provide their personal information in order to acquire cryptocurrencies or exchange them for fiat money using an exchanger. The exchangers must pass their users' personal information to the tax authorities.

The European Union: AMLD5

The regulatory approach taken by the European Union has been to address cryptocurrencies and the participants of the cryptocurrency market within the rules on money laundering and terrorist financing. The aim of Directive 2018/843, commonly referred as AMLD5 and which modified Directive 2015/849 (AMLD4), is: to increase transparency about the ownership of legal entities in order to prevent money laundering and terrorist financing via opaque arrangements or structures; to give financial regulators better access to information via centralised bank account registers; to tackle terrorist financing, money laundering, and tax evasion risks linked to the anonymous use of cryptocurrencies; and to improve the exchange of information between anti-money laundering supervisors and the ECB.

Unlike FATCA, AMLD5, which came into force on 10 January 2020, clearly defines cryptocurrencies within its scope. The commission took the approach of including both cryptocurrency exchanges and custodian wallet providers within the scope of AMLD5 and stated that they are obligated entities. In addition, the directive requires them: to conduct customer due diligence controls when exchanging cryptocurrencies, ending the anonymity associated with such exchanges and such wallet providers; to register with the relevant authorities; and to prepare suspicious activity reports when the situation warrants it. One remarkable aspect of AMLD5 is that it places greater emphasis on transparency in relation to ultimate beneficial ownership (UBO). Under AMLD5, European Union member states are asked to maintain interconnected, publicly available, national UBO registries which, in combination with the due diligence, the reporting of suspicious activity, and the registration of the cryptocurrency exchanges and wallet providers, provides them with access to valuable data that will help the tax authorities to mitigate risks and improve tax compliance in cryptocurrency transactions.

Article 2(1)(3) of AMLD5 includes the providers of virtual currency exchange for fiat currency services and the providers of custodian wallet providers as obligated entities that are within the scope of the directive, while Article 3(d)(18) and (19)

provide definitions of the terms “virtual currencies” and “custodian wallet providers” (Directive 2018/843). Consequently, and based on Articles 10 and 11 (Directive 2018/843), virtual currency exchange services and custodian wallet providers are subject to customer due diligence requirements. In addition, according to Article 47(1) (Directive 2018/843), they need to be licensed or registered. They are also obligated to report suspicious transactions to financial intelligence units. Article 13 states that they must identify the customer and verify their “identity on the basis of documents, data or information obtained from reliable and independent source” (Directive 2018/843). AMLD5 targets users indirectly if they utilise the services of a custodian wallet provider or enter into a cryptocurrency transaction via a cryptocurrency exchange platform. These users can no longer be anonymous because of the customer due diligence requirements applicable to custodian wallet providers and cryptocurrency exchange platforms that are detailed in the directive (Vandezande, 2018). At the same time, the information obtained during the process can be used by tax authorities to combat tax evasion. Articles 30 and 31 of AMLD5 (Directive 2018/843) list tax authorities among the competent authorities that must be granted access to the beneficial ownership register. This means that when transactions occur via a cryptocurrency exchange platform, the information will be available to the tax administration.

Problems with the European Union’s AMLD5

The existing European legal framework detailed in the AMLD5 (Directive 2018/843) does not cover the broader concept of cryptoassets—it just covers cryptocurrencies. Consequently, some participants in the cryptoasset market, such as token inventors and token offerors, are not within the scope of AMLD5 (Directive 2018/843). In addition, the directive fails to deal with the issues related to the identification of some of the participants behind cryptocurrency transactions and operations. There are no rules that unveil the anonymity of all stakeholders in the cryptocurrency market. As stated before, the key players in the cryptocurrency market are users, miners, cryptocurrency exchanges, trading platforms, wallet providers, inventors, and offerors. A number of these key players are not obligated entities under AMLD5 (Directive 2018/843). The greatest weakness of the approach taken in the directive is that suspicious transactions using cryptocurrencies made by stakeholders that are out of the directive’s scope are not well monitored by the authorities because they are unable to link identities and transactions in such cases (Houben & Snyers, 2018). Consequently, more substantive rules that could already have cryptocurrencies in their scope are not effective. This is especially true for the legal framework for the exchange of information in the field of international taxation. As an example, the EU’s framework on tax evasion relating to exit taxes is ineffective when it comes to cryptocurrencies because of their anonymous and easy-to-hide nature, something which is not solved by AMLD5 (Directive 2018/843). Users and miners are not obligated entities under the directive. Houben and Snyers (2018) state that, when proposing AMLD5, the European Commission submitted an impact assessment. They note that, according to this assessment, there are two main reasons for not considering miners to be obliged entities. The first one is that miners are considered to be providers of technical services instead of “gatekeepers” between the cryptocurrency market and the real world (Houben & Snyers, 2018, p. 76). The second is that, for the majority of cryptocurrencies, “miners are mostly located in China which would make any initiative largely impossible to enforce”

(Houben & Snyers, 2018, p. 76). In relation to cryptocurrency exchanges, they are classed as obliged entities under AMLD5 (Directive 2018/843). However, pure cryptocurrency exchanges are out of the scope of AMLD5 (Directive 2018/843) because they do not deal with fiat money. This means that atomic swaps, which are cryptocurrency for cryptocurrency exchanges, are out of the directive's scope (Houben & Snyers, 2018).

Houben and Snyers (2018) note that, in the case of trading platforms, no entities process or oversee the transactions that take place on them. In most cases, "they are operated exclusively by software (*i.e.* there is no central point of authority)" and this "makes it very hard to regulate them" (Houben & Snyers, 2018, p. 77).

They also distinguish three types of wallet provider: "hardware wallet providers", "software wallet providers" and "custodian wallet providers" (Houben & Snyers, 2018, p. 78). They point out that, of these, only custodian wallet providers "are obliged entities under AMLD5" (Houben & Snyers, 2018, p. 78). Finally, they state that coin offerors "are clearly not obliged entities under AMLD5" (Houben & Snyers, p. 78).

One may, therefore, ask if the AMLD5 (Directive 2018/843) framework achieves its goal to make cryptocurrency users and transactions transparent? Apparently not. As the mining business can be used for illegitimate purposes, pure cryptocurrency exchanges and, in most cases, trading platforms are out of its scope. Software and hardware wallet providers are also out of its scope as long as they do not exchange cryptocurrencies into fiat money, and coin offerors are not within its scope, leading to "blind spots" in the European Union's fight against tax evasion in relation to cryptocurrencies (Houben & Snyers, 2018, p. 79).

After analysing all of those problems and inconsistencies, the main question remains: how anonymous can transactions taking place within the cryptocurrency market still be after the implementation of AMLD5 (Directive 2018/843)? Should the directive be modified to incorporate the above-mentioned cryptocurrency market stakeholders as obligated entities in Article 2(1)(3) of the directive? Or would it be a better idea to ask them to take part in a voluntary registration scheme? Perhaps one of the biggest assumptions and lines of action that AMLD5 takes is to regulate the interaction between the so-called "virtual world" and the "real world" by trying to capture the jumps that users make between these worlds by exchanging cryptocurrencies for fiat money (or vice versa) in cryptocurrency exchanges, or the traditional storage of these currencies using wallet providers. A good starting point when attempting to improve the directive is to realise that, given the level of acceptance and the increasing use of cryptocurrencies, it is not necessarily true that users will want to exchange their cryptocurrencies for fiat money at some point. In fact, it is perfectly possible that they would prefer to keep them as cryptocurrencies and, perhaps, exchange them for other cryptocurrencies or use them as means of payment in the future. Incorporating this into the philosophy behind a future AMLD would lay the groundwork for including the actors that have so far been outside of the directive's scope. On the other hand, although AMLD5 (Directive 2018/843) seeks to target users through the compliance requirement of cryptocurrency exchanges and wallet providers, it could be an interesting starting point to improve the directive to include pure cryptocurrency exchanges and atomic swap transactions within its scope, while also including software and hardware wallet providers as obligated entities. With these two incorporations, the directive would fulfill its intended scope

since it would cover all possible types of cryptocurrency exchange and wallet provider. Houben and Snyers (2018) also suggest that a mandatory registry for all cryptocurrency users, miners, coin inventors, and coin offerors, whether individuals or legal entities, could be introduced. This would allow for a double check by the tax authorities. The regulation of miners and trading platforms seems to be a more complex task since, as mentioned before, most miners are outside of the European Union and trading platforms are operated by software and not by a central authority. From this point of view, a roadmap could start by including the stakeholders that are within the competences and inspection capabilities of the European Union while, at the same time, seeking to address the complex cases that have been mentioned through the exchange of information and coordination with different countries (Houben & Snyers, 2018).

United States: FATCA

FATCA has been the regulatory framework used by the United States to address the anonymity surrounding cryptocurrencies. Approved in March 2010, FATCA established an information communication regime for financial institutions in respect of certain accounts owned by U.S. citizens and residents. The approximation relies on the IRS's broad definition of the concept and understanding of what a foreign financial institution. FATCA's amended version of chapter 4, section 1471(d)(4) of the Internal Revenue Code of 1986 defines the term "foreign financial institution" as "any financial institution which is a foreign entity. Except as otherwise provided by the Secretary, such term shall not include a financial institution which is organized under the laws of any possession of the United States". The revised version of section 1471(d)(5) of the same chapter defines the term "financial institution" as: any entity that– "(A) accepts deposits in the ordinary course of a banking or similar business, "(B) as a substantial portion of its business, holds financial portion of its business, holds financial assets for the account of others, "(C) is engaged (or holding itself out as being engaged) primarily in the business of investing, reinvesting, or trading securities (as defined in section 475(c)(2) without regard to the last sentence thereof), partnership interests, commodities (as defined in section 475(e)(2)), or any interest (including a futures or forward contract or option) in such securities, partnership interests, or commodities."

The amended reporting requirements in Chapter 4, section 1471(b)(1) of the code, which apply "to any foreign financial institution if an agreement is in effect between such institution and the Secretary"[3], state that the institution must agree, amongst other things: "(A) to obtain information regarding each holder of each account maintained by such institution as is necessary to determine which (if any) of such accounts are United States accounts, "(B) to comply with such verification and due diligence procedures as the Secretary may require with respect to the identification of United States accounts, "(C) in the case of any United States account maintained by such institution, to report on an annual basis the information described in subsection (c) with respect to such account.

FATCA's amended version of Chapter 4, section 1471(c)(1) of the code details what a foreign financial institution has to report in respect of each U.S. account that it maintains. This information includes the U.S. account holder's name, address, Tax Identification Number (TIN), account number, and balance.

The United States uses FATCA to obtain information about the cryptocurrency accounts that its nationals have abroad, relying on the broad definition of the

concept of foreign financial institution that is present in FATCA and makes it possible to accommodate the inclusion of cryptocurrency exchanges and wallet providers (Valeriane, 2016).

Problems with the United States' FATCA

Although FATCA provides definitions for concepts such as U.S. account, financial account, and financial institution, its scope is broad and allows for different interpretations. The ambiguity and inaccuracy of FATCA in respect of the terms used and the lack of clarity on this aspect by the IRS has generated a climate of uncertainty among U.S. taxpayers. FATCA does not explicitly require cryptocurrency exchanges and wallet providers to report U.S. accounts (Valeriane, 2016). Valeriane (2016) notes that scholars and professionals are, in fact, unable to agree about whether the virtual market is included in FATCA or not. She states that "some argue that virtual wallets or exchanges would never enter into an agreement with the IRS because the virtual market is too different from the financial system" (Valeriane, 2016). Others argue "that there are certain exchanges that might be subject to reporting, while others assume that certain government agreements already include virtual currency exchanges" (Valeriane, 2016). In addition, there is no clarity about whether the broader concept of cryptoassets, particularly as it relates to tokens, falls within the concept of security and, consequently, within the scope of FATCA (European Commission, 2021).

On the other hand, the application of FATCA in its current wording generates a double legal qualification for cryptocurrencies, as the IRS qualifies them as property for the purposes of tax legislation but assimilates them to financial assets to enable the application of FATCA. The complexities that this interpretability can generate includes not only the fact that agreements based on cryptocurrencies may not materialise, but also that governments or financial institutions that already have agreements with the IRS may not be sure about their cryptocurrency reporting responsibilities.

The United States has, to date, taken the approach of obtaining data through appropriate exchange of information procedures with other tax authorities and financial institutions, and intends to use these intergovernmental agreements to implement FATCA as a mechanism via which to obtain information related to the use of cryptoassets held by other tax authorities and financial institutions. The fact that the terminology used in FATCA does not expressly refer to cryptoassets could pose an obstacle to the effectiveness of that instrument. It would be advisable to modify the regulation and make a concrete reference to cryptoassets. It would be desirable for the IRS to dispel the ambiguity by explicitly including the cryptoasset market within the scope of the regulation, by making express references to cryptocurrency exchanges and wallet providers, and by considering the stakeholders of the cryptoasset market who, until now, have been excluded, such as miners, coin inventors, coin offerors, and trading platforms.

Recent Public Consultations and Proposed Cryptoasset Legislation

The proposed AMLD6 clarifies 22 "predicate offences" that constitute money laundering and illicit finance, and aims to harmonise EU law on the subject within EU member states. In addition, it proposes to extend the liability to include both legal persons and individuals. With this in mind, it expands the traceability requirements for cryptoassets, and puts pressure on custodian wallet providers and cryptoasset

exchanges and their leaders to ensure that their staffs are properly trained to identify the risks associated with money laundering and terrorist financing with regard to cryptoassets. At the same time, it increases the associated penalties and lays the groundwork for the creation of an EU-based authority to counter money laundering and the financing of terrorism.

On the other hand, the European Commission launched a public consultation in 2021 with the aim of strengthening the rules on administrative cooperation and expanding the exchange of information regarding cryptoassets. In order to create a comprehensive framework for the reporting of cryptoassets, the European Commission tried to engage all cryptoasset market stakeholders in its public consultation (European Commission, n.d.). The public consultation, which collected important information regarding the cryptoasset market and stakeholders involved, resulted in the DAC8 proposal. According to Ahmed (2021), the aim of DAC8 is to "shed light on the virtual world", where "cryptoassets remain excluded from the purview of tax authorities" (p. 492). In its wording, the proposed DAC8 states that local tax authorities must be able to access the information so that they can share it with other tax authorities to enable domestic and cross-border cooperation (European Commission, 2022). DAC8 seeks to address cryptoasset anonymity from a tax administration perspective and proposes a coordinated set of rules in order to do so. In that context, DAC8 tries to solve the important challenges seen in AMLD5 by imposing mandatory reporting requirements for all relevant cryptoasset stakeholders and ensuring that they are classed as obligated entities.

If adopted, DAC8 will enhance the current framework at European Union level but will not address the anonymity issue from a global perspective in a virtual world where cryptoassets don't have borders.

A similar approach has been taken by the OECD with its 2022 public consultation, in which it is stated that the main purpose of the Cryptoasset Reporting Framework (CARF) is to "modernise the tax transparency of instruments available to tax administrations" (OECD, 2022, p. 3). The OECD (2022) intends to develop "a new global transparency framework which provides for the automatic exchange of tax information on transactions in Crypto-Assets in a standardised manner" (p. 3). In addition, it is taking the opportunity to propose changes to the common reporting standard (CRS) in order to better reflect the reality of the cryptoasset market when it comes to new financial assets and products (OECD, 2022).

Time will tell if the proposed legislation or the outcome of the public consultation will be adopted but what is clear is that, again, there is no unified approach to cryptoassets at the global level or how to approach the anonymity that surrounds them. The European Union is leading the regulatory efforts but the OECD is preparing what might be a global approach.

DISCUSSION

As has been addressed in this article, there is no single approach when it comes to regulating cryptoassets. Countries have taken different regulatory approaches with respect to cryptocurrencies, both in the way in which they are classified (either as property, private money, or foreign currency) and in terms of the tax consequences of cryptocurrency transactions (how to determine the cost and value at the time of alienating, whether or not there are capital gains, whether or not they are within the scope of VAT, or whether or not they are tax exempt). This undoubtedly creates tax planning opportunities as a result of hybrid mismatches

within different jurisdictions, which can allow taxpayers to find schemes that allowthem to avoid tax. On the other hand, until now, the approaches taken have depended on national legislation, which means that there is no consensus on how to solve the biggest problem that cryptocurrencies generate from a tax perspective: anonymity.

The different approaches taken by countries to regulate the anonymity of cryptocurrencies, together with initiatives such as those introduced by the United States through FATCA and the European Union through the AMLD5—regulations that, as previously discussed, leave key stakeholders out of the regulatory framework when it comes to covering the entire spectrum of the cryptocurrency market and bringing anonymity to transparency—added to the fact that the vast majority of countries lack regulations that seek to attack the anonymity of cryptocurrencies, generates a problem of great proportions which enables tax evasion.

In that sense, the heterogeneity within cryptocurrency regulations generates a two-layer problem. On the one hand, from a tax planning perspective, it is possible for taxpayers to find tax planning structures that allow them to minimise the tax base based on the mismatches between countries in terms of the characterisation and classification of cryptocurrencies. This can, undoubtedly, be a problem from a tax justice and tax collection perspective, but it is far from being the biggest problem that exists. On the other hand, the central and critical problem—the lack of regulation and coordination within and between countries with regard to how to address the anonymity of cryptocurrencies in particular, and cryptoassets in general, enables (or makes it nearly impossible to detect) tax evasion in specific countries and between different jurisdictions.

What could the solution to this tax evasion be given the lack of regulation and coordination? Could asking taxpayers and cryptocurrency market participants to take part in a voluntary register scheme in order to declare their activities be an alternative? Or would it be better to make participation in such a scheme mandatory? Trusting in a voluntary register scheme to achieve the unveiling of anonymity is not a workable solution. Taxpayers have little to no incentive to voluntarily report something that is not likely to be detected. So, in such a scenario, how can the tax authorities detect a breach if there is no coordination between countries and the cryptoasset market is an electronic worldwide market without borders? Is this at all possible when pseudonymous cryptoassets are concerned and different regulations fail to cover all stakeholders in the cryptoasset market? Does it make sense to ban cryptoassets and declare them illegal? On the one hand, it is possible to argue that it is not, since it would not be possible to know who owns them anyway. On the other hand, it is possible to argue yes, since there would be an inhibiting factor and laws in place with which to prosecute cryptoasset market participants.

Every tax administration faces more or less the same problems with regard to the anonymity of cryptoassets, but they take different approaches to solving them, which creates the opportunity for misunderstandings, mismatches, arbitrages, tax evasion, and tax planning to take place. So why the use of different solutions? What is clear, at least, is that if every country takes its own regulatory approach to the characterisation of cryptoassets and how to deal with their anonymity, the problems mentioned so far will continue to exist. Does it make sense then to take a common approach? Since cryptoasset transactions and the stakeholders of the cryptoasset market are not bound by borders, at which level should this issue be tackled? Is there space for international coordination in the matter? If yes, what are the options?

Are the efforts made by the European Union, with the proposed DAC8, and the OECD, with its public consultation about the CARF, the right approach? Should this be expanded to have as many countries involved as possible? All these questions allow for further and required research.

CONCLUSIONS

During the past few years, there has been a dramatic increase in the use of cryptoassets worldwide. Today, there are more than ten thousand different cryptocurrencies, and technological progress and innovation has led countries to broaden the concept of cryptoassets, and to question their treatment from regulatory and tax perspectives. Currently, there is no consensus at the country level on the regulatory treatment of cryptoassets. Countries have taken different regulatory approaches with respect to cryptoassets such as cryptocurrencies, both in respect of how they classify them (either as property, private money, or foreign currency) and in terms of the tax consequences of cryptoasset transactions (e.g. how to determine their cost and value at the time of alienating, whether or not there are capital gains, whether or not they are within the scope of VAT, or whether or not they are tax exempt).

This article focusses on a broader concept by analysing cryptoassets and the tax administration issues related to the anonymity surrounding them. From a tax perspective, the biggest challenge posed by cryptoassets is anonymity. When a tax administration does not know who is behind a transaction due to the anonymity that surrounds cryptoassets, it loses its role as a tax compliance watchdog and cannot sanction such tax evasion. Every tax administration faces more or less the same problem, but they take different approaches. In the case of the United States, the IRS decided to use FATCA to address the anonymity behind cryptocurrencies, but this has caused problems due to legal uncertainty. FATCA does not explicitly require cryptocurrency exchanges and wallet providers to report U.S. accounts. In fact, scholars and professionals are unable to agree about whether the virtual market is included in FATCA or not. On the other hand, the application of FATCA in its current wording generates a double legal qualification for cryptocurrencies, as the IRS qualifies them as property for the purposes of tax legislation but assimilates them to financial assets to enable the application of FATCA. The European Union, for its part, through AMLD5, has tried to combat the anonymity of cryptocurrencies in order to prevent money laundering, terrorist financing, and tax evasion but, as was shown in this article, that legislation has not covered all cryptocurrency market stakeholders and does not cover the broader concept of cryptoassets, making its effectiveness questionable.

Does it make sense for countries to take a common approach to tackle this problem? Since cryptoasset transactions and cryptoasset market stakeholders are not bound by borders, as long as there is no single approach taken and the treatments that countries apply to cryptoassets differ as much as they do today, there will always be ways to arbitrate, evade taxes, and take non-legitimate advantages through the use of cryptoassets. At which level should this issue be tackled? Is there space for international coordination in the matter? If yes, what are the options? Are the European Union's DAC8 and AMLD6, and the OECD's public consultation about the CARF, the correct approach? Time will tell, but what is clear is that there is a need for a unified approach to be taken at the global level in order to tackle cryptoasset anonymity.

REFERENCES

Ahmed, M. (2021). Cryptocurrency tax compliance in the European Union: Reality or mirage? European Taxation, 61(11). https://doi.org/10.59403/2hchvwm

Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., & Capkun, S. (2013). Evaluating user privacy in Bitcoin. In A. R. Sadeghi (Ed.), Lecture notes in computer science: Vol.7859: Financial cryptography and data security, FC2013 (pp. 34–51). Springer. https://doi.org/10.1007/978-3-642-39884-1_4

Annunziata, F. (2020). Speak, if you can: What are you? An alternative approach to the qualification of tokens and initial coin offerings. European Company and Financial Law Review, 17(2), 129–154. https://doi.org/10.1515/ecfr-2020-0007

Bal, A. M. (2013). Stateless virtual money in the tax system. European Taxation, 53(7), 351– 356.

Bal, A. (2014a). Should virtual currency be subject to income tax? SSRN. https://doi.org/10.2139/ssrn.2438451

Bal, A. M. (2014b). Taxation of virtual currency (Meijers-reeks) [Doctoral dissertation, University of Leiden]. Institutional Repository of the University of Leiden. https://hdl.handle.net/1887/29963

Bal, A. M. (2015). Bitcoin transactions: Recent tax developments and regulatory responses. Derivatives & Financial Instruments, 17(5), 1–10.

Bal, A. (2019). Developing a regulatory framework for the taxation of virtual currencies. Intertax, 47(2), 219–233. https://doi.org/10.54648/taxi2019019

Byrnes, W. H., & Munro, R. J. (2015). Money laundering, asset forfeiture and recovery, and compliance—A global study guide. Matthew Bender Elite Products.

Cumming, D. J., Johan, S., & Pant, A. (2019). Regulation of the crypto-economy: Managing risks, challenges, and regulatory uncertainty. Journal of Risk and Financial Management, 12(3), Article 126. https://doi.org/10.3390/jrfm12030126

Directive 2015/849. 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, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC. European Union. http://data.europa.eu/eli/dir/2015/849/oj

Directive 2018/843. 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. European Union. http://data.europa.eu/eli/dir/2018/843/oj

European Central Bank. (2015). Virtual currency schemes – A further analysis. European Central Bank. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

European Commission. (n.d.). Tax fraud & evasion — Strengthening rules on administrative cooperation and expanding the exchange of information: Have your say. European Commission. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12632-Tax-fraud-evasion-strengthening-rules-on-administrative-cooperation-and-expanding-the-exchange-of-information_en

European Commission. (2021). Proposal for a directive of the European parliament and of the council on the mechanisms to be put in place by the member states for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and the repealing directive (EU) 2015/849, COM(2021) 423 final. European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021PC0423

European Commission. (2022). Council directive amending directive 2011/16/EU on administrative cooperation in the field of taxation, COM(2022) 707 final. European Commission. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12632-Tax-fraud-evasion-strengthening-rules-on-administrative-cooperation-and-expanding-the-exchange-of-information_en

European Securities and Markets Authority. (2019). Advice: Initial coin offerings and crypto- assets. ESMA. https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf

European Union. (2006). Council directive 2006/112/EC of 28 November 2006 on the common system of value added tax. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0112

Financial Action Task Force. (2014). Virtual currencies: Key definitions and potential AML/CFT risks. FATF. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual- currency-key-definitions-and-potential-aml-cft-risks.pdf

The Foreign Account Tax Compliance Act, 2010.

Grinberg, R. (2011). Bitcoin: An innovative alternative digital currency, Hastings Science & Technology Law Journal, 4(1), 160–208.

He, D., Habermeier, K., Lecklow, R., Haksar, V., Almeida, Y., Kashima, M., Kyriakos-Saad, N., Oura, H., Sedik, T. S., Stetsenko, N., & Verdugo-Yepes, C. (2016). Virtual currencies and beyond: Initial considerations (IMF staff discussion note SDN/16/03). International Monetary Fund. https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf

Hellani, H., Samhat, A. E., Chamoun, M., Ghor, H. E., & Serhrouchni, A. (2018). On blockchain technology: Overview of Bitcoin and future insights. Proceedings of the 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET). IEEE. https://doi.org/10.1109/IMCET.2018.8603029

Herlin-Karnell, E., & Ryder, N. (2017). The robustness of EU financial crimes legislation: A critical review of the EU and UK anti-fraud and money laundering scheme. European Business Law Review, 28(4), 427–446.

https://doi.org/10.54648/eulr2017023

Herrera-Joancomartí, J. (2014). Research and challenges on Bitcoin anonymity. In J. Garcia- Alfaro, J. Herrera-Joancomartí, E. Lupu, J. Posegga, A. Aldini, F, Martinelli, & N. Suri (Eds.), Lecture notes in computer science (including subseries Lecture notes in artificial intelligence and lecture notes in bioinformatics): Vol. 8872: Data privacy management, autonomous spontaneous security, and security assurance, 9th international workshop, DPM 2014, 7th international workshop, SETOP 2014, and 3rd international workshop, QASA 2014, Wroclaw, Poland, September 10-11, 2014: Revised selected papers (pp. 3–16). Springer. https://doi.org/10.1007/978-3-319-17016-9_1

Houben, R., & Snyers, A. (2018). Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion. European Parliament. https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

Houben, R., & Snyers, A. (2020). Cryptoassets: Key developments, regulatory concerns and responses. European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf

Kaplanov, N. M. (2012). Nerdy money: Bitcoin, the private digital currency, and the case against its regulation. Loyola Consumer Law Review, 25(1), 111–174.

Koshy, P., Koshy, D., & McDaniel, P. (2014). An analysis of anonymity in Bitcoin using P2P network traffic. In N. Christin & R. Safavi-Naini (Eds.), Lecture notes in computer science: Vol. 8437: International conference on financial cryptography and data security, FC 2014 (pp. 469–485). Springer. https://doi.org/10.1007/978-3-662-45472-5_30

Langer, M. (2017, December 20). Taxation of cryptocurrencies in Europe. Crypto Research Report. https://cryptoresearch.report/crypto-research/taxation-cryptocurrencies-europe/

Lewis, R., McPartland, J., & Ranjan R. (2017). Blockchain and financial market innovation. Economic Perspectives, 41(7). https://www.chicagofed.org/publications/economic-perspectives/2017/7

Marian, O. (2013). Are cryptocurrencies super tax havens? Michigan Law Review First Impressions, 122, 38–48.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. SSRN. https:/doi.org/10.2139/ssrn.3440802

Natarajan, H., Krause, S., & Gradstein, H. (2017). Distributed ledger technology (DLT) and blockchain (FinTech Note, Note 1). International Bank for Reconstruction and Development/The World Bank. http://documents.worldbank.org/curated/en/177911513714062215/Distributed-Ledger-Technology-DLT-and-blockchain

Ober, M., Katzenbeisser, S., & Hamacher, K. (2013). Structure and anonymity of the

Bitcoin transaction graph. Future Internet, 5(2), 237–250. https://doi.org/10.3390/fi5020237

Organisation for Economic Co-operation and Development. (2018). Tax challenges arising from digitalisation – Interim report 2018: Inclusive framework on BEPS (OECD/G20 base erosion and profit shifting project). OECD Publishing. https://doi.org/10.1787/9789264293083-en

Organisation for Economic Co-operation and Development. (2020). Taxing virtual currencies: An overview of tax treatments and emerging policy issues. OECD Publishing. https://www.oecd.org/tax/tax-policy/taxing-virtual-currencies-an-overview-of-tax- treatments-and-emerging-tax-policy-issues.pdf

Organisation for Economic Co-operation and Development. (2022). Crypto-asset reporting framework and amendments to the common reporting standard: Public consultation document: 22 March – 29 April 2022. OECD Publishing. https://web-archive.oecd.org/2022-03-22/627496-public-consultation-document-crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.pdf

Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the Bitcoin system. In Y. Altshuer, Y. Elovici, A. B. Cremers, N. Aharony, & A. Pentland (Eds.), Security and privacy in social networks (pp. 197–223). Springer.

Snyers, A., & Pauwels, K. (2018). ICOs in Belgium: Down the rabbit hole into legal no man's land? Part 1. International Company and Commercial Law Review, 29(8), 491–510.

Spagnuolo, M., Maggi, F., & Zanero, S. (2014). BitIodine: Extracting intelligence from the Bitcoin network. In N. Christin & R. Safavi-Naini (Eds.), Lecture notes in computer science: Vol. 8437: International conference on financial cryptography and data security, FC 2014 (pp. 457–468). Springer. https://doi.org/10.1007/978-3-662-45472-5_29

Valeriane, E. M. (2016). IRS, will you spare some change? Defining virtual currency for the FATCA. Valparaiso University Law Review, 50(3), 863-911.

Vandezande, N. (2018). Virtual currencies: A legal framework. Intersentia.

Witzig, P., & Salomon, V. (2018). Cutting out the middleman: A case study of blockchain- induced reconfigurations in the Swiss financial services industry (Working Paper 1, 2018/E, The circulation of wealth). Université de Neuchâtel. https://libra.unine.ch/bitstreams/d60c453b-3adf-498a-a91e-4b41ef9a282d/download