Common Reporting Standard: the blockchain-based assets case

by

FERNANDEZ-LEENKNECHT TRANG

I. Introduction

1.1 Objectives of the master thesis

In 2014, the OECD and G20 countries together with the EU[1] developed the new global model for Automatic Exchange of Financial Account Information in Tax Matters[2] (AEoI) to facilitate cross-border tax transparency on financial accounts held abroad and intends to equip tax authorities with an effective tool to tackle offshore tax evasion by providing a greater level of information[3]. The Common Reporting Standard (CRS) contains the reporting and due diligence standard that underpins the AEoI[4]. AEoI, beneficial ownership (BO) registration, and tax administrations may undergo a revolutionary development thanks to the blockchain technology[5]. Benefits are expected to help to reduce the number of intermediaries, improving transparency and increasing security in policy. It is essentially a system to encrypt information and a shared database, based on a consensus mechanism amongst trusted parties to certify the information and validate transactions without a central authority to authenticate the information[6]. Automatic information reporting models such as US Foreign Account Tax Compliance Act (FATCA) and AEoI/CRS were developed based on years of experience in 'traditional' financial services. Blockchain, tech service providers and blockchain-based assets ('crypto') are new, and regulators struggle to understand with how they work. Measures for the crypto business should be tailored to address the unique risks and challenges of the crypto market. The objective of this paper is to analyse the application of CRS for AEoI purposes in light of the spectacular rise of cryptoassets in the economic and tax spheres and explore possible paths for solutions within the scope of the OECD BEPS[7] Project.

---

1 Organisation for Economic Co-operation and Development respectively European Union.

2 Standard for Automatic Exchange of Financial Account Information in Tax Matters, Second Edition, OECD Publishing, Paris.

3 www.oecd.org/tax/automatic-exchange (last visit 9.6.2019).

4 See Standard for AEoI, Introduction #19. Directive 2014/107/UE of 9.12.2014, commonly referred as DAC2, which is almost a copy of CRS.

5 IBFD, Digital Economy, Dispute Resolution & Blockchain Technology dominate 12th edition of IFA Mauritius conference, 24.5.2018.

6 Swiss Federal Council, Legal framework for blockchain and distributed ledger technology (DLT) in the financial sector, Introduction #2.1, Bern, 14.12.2018.

7 The Inclusive Framework on Base Erosion and Profit Shifting.

1.2 Common Reporting Standard for AEoI purposes

CRS was designed to be under the umbrella of the OECD Multilateral Convention of Administrative Assistance in Tax Matters[8] (MCAATM) and through the execution of the CRS Multilateral Competent Authority Agreement (MCAA[9]) or bilateral CAA. It calls on jurisdictions to obtain information from their financial institutions (FIs) and automatically exchange that information with other jurisdictions on a routine basis[10] in order to help to determine which country has taxing jurisdiction over assets without relying on taxpayers' self-disclosure. The objective is to identify taxpayers who hold assets in financial accounts outside their home jurisdictions. CRS provides that certain FIs collect financial information on their clients, as long as they are resident abroad for tax purposes (tax residency). It expounds the FIs required to report, the financial account information to be exchanged, the types of accounts and taxpayers covered, as well as due diligence procedures to be followed by FIs. This information covers all types of investment income and account balances[11]. As a rule, this information is automatically transmitted once a year to the tax authority, which transmits the data for the client to the respective tax authority abroad[12]. This transparency seeks to prevent tax bases from being hidden from the tax authorities abroad. Aside from Switzerland, 128 states and territories, including all major financial centres, have declared their intention to adopt the AEoI[13]; participating jurisdictions have commenced exchanges in 2017 or 2018.

1.3 Characteristics of blockchain-based assets

The blockchain technology was developed a decade ago nonetheless without large-scale tangible application. In recent years, the surge of cryptocurrencies has gained increased attention to the technology from both the private sector and the authorities. Blockchain-based assets, commonly referred to as

---

8 In particular articles 4 and 6. European Commission, Administrative cooperation in (direct) taxation in the EU (ec.europa.eu, last visit 28.8.2019).

9 61 jurisdictions signed the MCAA (as of 7.6.2019).

10 Background, OECD (2018), Standard for Automatic Exchange of Financial Information in Tax Matters - Implementation Handbook – Second Edition, OECD, Paris.

11 See Standard Implementation, Introduction #9.

12 Global Forum, Background information brief, January 2016.

13 SIF, Financial Accounts (last visit 28.3.2019). OECD portal (last visit 7.6.2019).

cryptoassets, are "natively digital[14]", in the sense of they are not issued by any central authority, and the technology guarantees that data recorded in the registry are theoretically immune to government interference, manipulation or counterfeit. In fact, the distinctive feature of cryptoassets is the lack of an underlying claim/liability, from which they derive their specific risk profile. Units of a cryptoasset may be used as a means of exchange and are *de facto* considered by their users as assets, i.e. 'something of value[15]'. Bitcoin, the world's most popular cryptocurrency[16], has the potential to become a store of value and an alternative to traditional asset classes. Other features of Blockchain are the 'tokenization' of assets in an initial coin offering (ICO) for ease of transfer across borders and the 'mining' of tokens. This blockchain technology was initially outside the scope of the OECD and not part of BEPS plan as scholars and policymakers have been pondering over whether cryptoassets are 'real' currencies setting up a new global payment and value standard.

1.4 Scope of the thesis

CRS sets out the FIs required to report and the taxpayers covered, that includes the need to establish the identity of accountholders and asset BOs. In principle information exchanged cannot be used by authorities for non-tax purposes (e.g. to tackle corruption or money laundering). At its core, Blockchain allows to record assets, transfer value and track transactions, ensuring the transparency, integrity and traceability of data in a decentralised manner. Yet, Bitcoin may develop into a potential offshore tax avoidance heaven[17] thanks to the use of this cryptocurrency on decentralised exchanges to buy a wide variety of tokenised securities and assets in an anonymous manner.

This thesis will examine the hurdles of the AEoI under CRS for blockchain-based assets and income, and how an accountholder, or a 'walletholder', should account for AEoI purposes. The *next section* addresses the application of AEoI in the traditional financial system. It analyses the concepts and the

---

14 KPMG, Institutionalistion of cryptoassets, "Introduction", November 2018.

15 P.8, European Central Bank (ECB) Crypto-Assets Task Force, Occasional Paper Series, Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures, No 223/May 2019.

16 Out of more than 2000 cryptocrrencies. P.4, European Securities and Markets Authority (ESMA) Advice Initial Coin Offerings and Crypto-Assets, ESMA50-157-1391, 9.1.2019.

17 Michael Ou, Overreach or Necessary Correction? Why FATF Guidelines on Blockchain Are a Good First Step, Nasdaq, 13.8.2019.

information required under CRS. It also sets out the interactions between the tax administration of the taxpayer residence state and the foreign tax administrations. The *third section* examines CRS and the case of blockchain-based assets, and explores its possible approaches. The *fourth section* provides an overview of current developments of government actions in selected countries to address and ensure tax compliance of cryptousers and service providers.

II. Application of CRS for AEoI purposes

Many jurisdictions already exchange information automatically with their contracting partners on various categories of income as well as other types of information[18] such as change of residence, operation on immovable property, tax withheld at source. The CRS protocol sets out a minimum standard and does not intend to restrict the other types of AEoI[19]. States may choose to go beyond the minimum standard[20]. The OECD's protocol consists of two main parts: CRS, which contains the reporting and due diligence rules to be imposed on FIs, and the Model CAA, which contains the detailed rules on the AEoI[21].

2.1 The 'traditional' financial system

To prevent taxpayers circumventing the AEoI Model by shifting assets to institutions or investing in products that are not covered by the Model, a comprehensive reporting regime requires a broad scope across three dimensions: the financial information to be reported, the accountholders subject to reporting, and the FIs required to report. Hence, the Model involves the systematic and periodic transmission of "bulk" tax data by the source country to the residence country[22] (Figure 1). FIs report information of financial assets hold on behalf of non-resident taxpayers to the tax administration in the jurisdiction they are located. This includes all types of income, account balances, account and tax identification number (TIN), names, addresses and taxpayers' dates of

18 Such as the bilateral "Protocol of Amendment to the Agreement on the Taxation of Savings Income" of 27.5.2015 between Switzerland and the EU.

19 See Standard Implementation, Annexe 3, Introduction.

20 Federal Department of Finance, SIF's position of 16.4.2018 on the introduction of disclosure rules for intermediaries along the lines of the OECD model rules.

21 See Background information brief. The full version, as approved by the OECD on 15.7.2014, includes the Commentaries on the Model CAA and the CRS, and seven annexes.

22 See Standard for AEoI, Annex 3, Introduction.

birth. The tax administrations annually transmit that information to the jurisdiction(s) of residence of the taxpayers.

A. Concepts and information covered under CRS

A comprehensive reporting regime covers:

– Financial institutions that need to report, such as custodial and depository institutions, brokers and investment entities, traders in securities, certain collective investment vehicles and specified insurance companies, corporate trustees, and intermediaries managing assets on behalf of others[23];

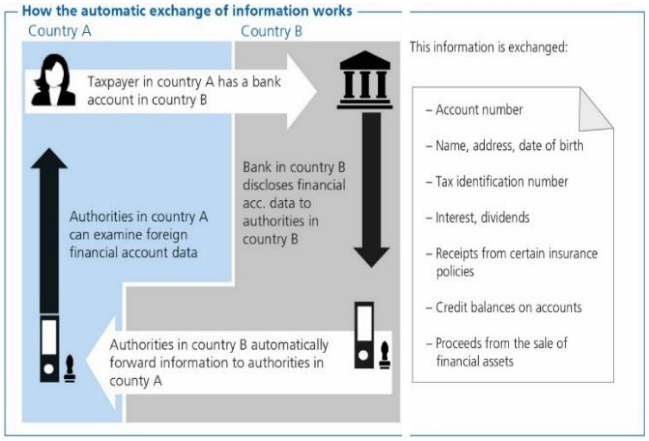

Figure 1. AEoI framework for reciprocal exchange under the CRS
© EFD/DFF

– Financial information to be exchanged with respect to reportable accounts, such as account balances and value, all types of investment income, sales proceeds from financial assets, other income transferred, paid or generated with respect to assets held in the account[24];

– Reportable accounts held by reportable persons, i.e. individuals and legal entities including trusts and foundations, that are resident for tax purposes in a reporting jurisdiction. Pursuant to FATF[25], passive entities are subject to a look-through obligation[26] which exposes the individuals that ultimately control or own these legal entities and/or on whose behalf a transaction or activity is conducted, i.e. the BOs[27].

---

23 See Standard for AEoI, Introduction #20.
24 See Standard for AEoI, Foreword.
25 Financial Action Task Force. See Standard for AEoI, B. CRS, Section VII (D, 6).
26 Passive non-financial entities (NFE). See p3, Background information brief.
27 Art. 3(6) of the 4th AMLD.

CRS also describes the due diligence procedures to identify reportable accounts and obtain the accountholder identifying information[28].

B. Allocation of taxing rights and effective taxation

With the introduction of the Model, participating jurisdictions will receive unrequested bank account related information from other contracting States. National authorities are entitled to use this information. The main benefit of AEoI is the subsequent effective taxation by the states where taxes should have been paid according to the allocation keys of taxing rights based on applicable tax treaties and domestic laws[29]. The AEoI can:

– provide timely information on non-compliance where tax has been evaded either on an investment return or the underlying capital sum;

– help detect cases of non-compliance even where tax administrations have had no previous indications of non-compliance;

– increase tax revenues and ensure that all taxpayers pay their fair share of tax in the right place at the right time;

– educate taxpayers in their reporting obligations.

The first AEoI took place in September 2017 among the early adopter states. Switzerland exchanged information with 36 partner states in autumn 2018 after data collection during 2017. The deterrent effects of the forthcoming global AEoI flooded the tax administrations with massive numbers of voluntary disclosure actions introduced by taxpayers, often also incentivised by 'tax amnesty' programmes introduced by several governments[30]. On 7 June 2019[31] an OECD study reported a 34% decline on deposits in offshore accounts between 2008 and 2018 from a peak of USD 1.6 trillion when the financial crisis broke out. About 65% of the decrease would account for the onset of CRS. Over the 2009-2019 period voluntary disclosure of offshore accounts, financial assets and income resulted in more than EUR 95 billion in additional revenue (tax, interest and penalties) for OECD and G20 countries[32].

---

28 See point 2.1 Background information brief, #10.

29 Notwithstanding possible penalties and other measures by the authorities.

30 RTS Info, Les cantons romands croulent sous les dénonciations spontanées, 17.5.2017.

31 OECD Exchange of Information portal, Implementation of tax transparency initiative delivering concrete and impressive results, 7.6.2019.

32 Le Monde, L'OCDE constate une importante décrue des dépôts bancaires dans les paradis fiscaux, 7.6.2019. See also Standard for AEoI Commentary Article 6 #63.

2.2 Interactions in the taxpayer residence state

The Model needs to be implemented by participating jurisdictions[33], whose process can be summarised in four main steps[34], in any order or pursued in parallel: 1) translate the reporting and due diligence requirements into domestic laws; 2) select a legal basis; 3) set up the IT and administrative capabilities to receive and exchange information by the reporting entities; and 4) ensure the highest standards of confidentiality and data safeguards. Reporting FIs' obligations have to: a) register with the competent authority; b) identify Reportable Financial Accounts; and c) collect information with respect to an accountholder's country of residence/domicile. The due diligence requirements distinguish between Pre-Existing and New Accounts as well as between individual accounts and accounts of legal entities. FIs are also required to identify a Reportable Person, based on the available information (AML/KYC procedure) and determine whether an Entity is a passive NFE and, if so, the identity and domicile of Controling Persons. Jurisdictions have discretion over whether to allow FIs to apply a threshold of USD 250'000, under which Preexisting Entity Accounts need not to be reviewed. In Switzerland, the legal basis for the AEoI Model comprise the MCAATM, the MCAA and the Swiss AEoI Act together with the AEoI Ordinance[35] in force since 2017. The Federal Tax Administration's (FTA) guidelines set out the standards for implementation by FIs[36]. For the Model targets cross-border situations, domestic situations may not be affected[37].

2.3 Interactions with the foreign tax administrations

AEoI requires a preliminary agreement between contracting jurisdictions on the procedure to be adopted and on the items covered, whose fitness for exchange will depend on each State's own domestic administrative systems[38]. The agreement can be entered by two or more parties[39]. Switzerland usually implements the AEoI according to the MCAA, which must be followed by a

33 See Standard for AEoI, Introduction.
34 See Background information brief p4 with reference to the Handbook, part I, p12.
35 Swiss Federal Departement of Finance (FDF), Automatic exchange of information, 2.2019.
36 Swiss Bankers Association, Swiss Banking, AEoI (swissbanking.org/en/topics/tax/the-automatic-exchange-of-information#, last visit 10.6.2019).
37 E.g. the banking secrecy on Swiss bank accounts of taxpayers residing in Switzerland.
38 See Standard for AEoI, Commentary on art. 6 #65 with reference to art. 24.
39 Actual AEoI takes place on a bilateral basis. See Standard for AEoI, Introduction #11.

bilateral activation such as the joint declaration[40] (Figure 2). Bilateral treaties have been concluded with the EU, Hong Kong and Singapore[41]. Partner states for AEoI purposes are selected and approved[42] when they satisfy the exacting requirements in terms of data protection and the principle of speciality[43]. In addition, reciprocity[44] must be guaranteed as well as robust regulations for identifying the BOs of all types of legal entities, including trusts and domiciliary companies. Financial account information of natural persons or legal entities with Swiss bank accounts are transmitted to the tax authorities of their country of residence while Swiss tax authorities are being transmitted information on foreign accounts of Swiss taxpayers by the countries in which the financial accounts are located – providing such states are AEoI contracting states. The Global Forum[45] examines the domestic implementation of committing countries by means of peer reviews with the aim to create a global level playing field[46]. The peer reviews for Switzerland will start in 2020.

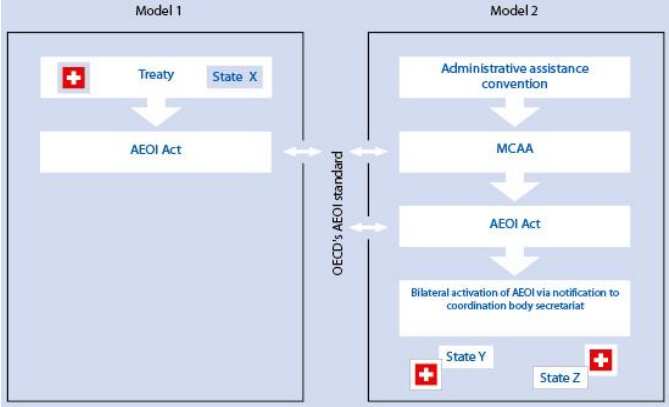

Figure 2. AEoI legal agreement framework. © EFD/DFF

III. Asset and income in a blockchain-based system

'Crypto' is defined broadly as digital units of account in which cryptographic techniques are used to regulate the generation and distribution of units on

40 Ex. Switzerland and Australia in March 2015.
41 SIF, Financial Accounts.
42 By January 2019, the Swiss Parliament has approved the introduction of the AEoI with 89 partner states, which include all EU/EFTA member states and almost all G20/OECD states. A further 19 partner states are to be added to Switzerland's network, and the AEoI should be implemented with them from 2020/2021 onwards. See FDF, AEoI, 29.5.2019.
43 Data may be used solely for tax purposes.
44 To Switzerland. Some jurisdictions agreed to not receive data from Switzerland (ex: BVIs).
45 Global Forum on Transparency and Exchange of Information for Tax Purposes.
46 www.oecd.org/tax/transparency/automaticexchangeofinformation (last visit 9.6.2019).

Blockchain[47] (coins or tokens). In practice, crypto means multiple things to different people: an investment asset class like commodities, a store of value like gold, a legitimate medium of exchange, a covert method of exchange, an immutable record of rights and ownership, or an incentive tool like rewards points. Although 'cryptoasset' covers a broader range than 'virtual currency' or 'cryptocurrency', they are used synonymously in this paper. In line with the scope of this thesis, and following FINMA's[48] focus on the function and transferability of tokens, only security-like tokens that function as an investment in economic terms will be addressed under the term cryptoassets'.

3.1 Cryptoassets: global payment and value standard

States and banks, despite their flaws and the resentment they inspire, have long played the role of guarantors and trusted intermediaries. A technical basis for numerous cryptocurrencies, Blockchain[49] was developed in response to the global financial crisis and the ensuing lost of trust in governments and the traditional financial system with the ambition to recreate this trust in an automated way. It relies exclusively on computer code to eliminate human arbitrariness. This new payment and value medium can bypass the traditional banking system by using the decentralised transaction model that is exclusively processed over Blockchain[50]. For the first time in history, every person with a smarthphone has access to a digital asset that is not tied to any country. Cryptoassets are "any form of virtual asset stored on an electronic medium that allows a community of users who accept them as means of payment to execute transactions in such assets without using a legal currency"[51]. They can be used across three functions[52]: payment purpose, usage purpose or investment purpose. Two types of products and services are emerging: the cryptoassets or tokens, and the infrastructure that enables the issuance (ICO, mining), facilitation (exchange, custody), and utility (store of value, ownership,

47 See Institutionalistion of cryptoassets, Introduction.

48 Swiss Financial Market Supervisory Authority.

49 The variety of systems developed in practice goes beyond Blockchain and is referred as DLT, a distributed ledger enforced by a disparate network of computers. See Legal framework, Index and p12.

50 And the distributed ledger technology (DLT). See CGMF, p35.

51 In other words, they can be digitally traded for real goods and services. Report of the interdepartemental Coordinating Group on combating Money laundering and the Financing of terrorism (CGMF), National Risk Assessment (NRA): Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding, "Introduction", October 2018.

52 See CGMF, Index.

rights) of these tokens[53]. The process of 'tokenisation' is rather easy, and more tokens will continue to proliferate in the ecosystem. While Bitcoin has its own denomination, it is usually not accepted as legal tender as opposed to 'fiat money', the fiduciary currencies that are issued by a state whose central bank sets and controls the legal rate.

The distributed nature enables transactions to be processed directly between the parties. It only requires the participants to agree on the transactions to be validated and a valid register, which functions as a distributed consensus. The validating consensus is performed by the so-called 'miners' all over the world, who can be individuals or companies. The work of mining is open to the entire ecosystem[54]: everybody can potentially participate and mine tokens. Miners' activity is compensated with new virtual currency as 'transaction fees'[55], which increases the overall volume of that cryptocurrency, equivalent with the printing of banknotes by a central bank. This means that virtual assets may not only *represent* 'something of value' but could be the things of value in *themselves*[56]. Under current EU laws, cryptoassets do not appear to fit under any of the subject matter-relevant EU legal acts[57]. As a consequence, cryptoassets and related activities are unregulated, with the exception of AML rules.

3.2 ICO and tokens

The operation of ICO can generally be seen as the creation of tokens, during which an issuer accepts fiat money or cryptocurrencies and issues tokens in return. The tokens are linked to the promise of consideration, that may take on very different forms. A token is "a unit that either contains an intrinsic value or represents another asset or a usage function[58]". It is usually fungible and can be exchanged between network users. Technology-neutral rules shall apply, to the extent possible, to the issuance, bookkeeping and use of these tokens as they apply to the financial values, they represent[59].

---

53 See Institutionalisation of cryptoassets, p8.

54 Favre/Houdrouge/Elsener, The Virtual Currency Regulation Review - Edition 1, Switzerland, Law Reviews, November 2018.

55 See CGMF, Index.

56 Securities have long existed in digital form through book entry systems. Max Ganado, Blockchain: Some legal considerations relating to Security Token Issuance, 12.7.2019.

57 See p28, ECB Crypto-Assets Task Force.

58 See CGMF, Index.

59 See p9, ECB Crypto-Assets Task Force.

At publication of FINMA's guidelines[60], there was neither in Switzerland or internationally recognised terminology for the classification of cryptoassets[61] or ICO[62]. In the main lines, the Swiss approach reflects European Securities and Market Authority's (ESMA) stand in assessing ICOs[63]. FINMA focus on the economic function and tradeability of tokens issued by the ICO issuer and bases its determination on the applicable legal definitions (Figure 3). The key factors are the underlying purpose of the tokens[64], which sets three types of tokens categories: payment tokens, utility tokens, and asset tokens. In assessing whether tokens are comparable to securities[65]:

– Payment tokens are synonymous with cryptocurrencies and can serve as means of payment. They differ in their function from traditional securities. They are treated as securities in pre-financing and pre-sale situations where the tokens do not yet exist but the claims are tradeable.

– Utility tokens are created to provide digital access to an application or service by means of a blockchain-based infrastructure. The utility token is treated as a security if at issuance it has an investment purpose[66];

– Asset tokens are regarded as participations in real physical underlyings, companies, or earnings streams, or an

	Pre-financing and pre-sale / The token does not yet exist but the claims are tradeable	The token exists
ICO of payment tokens	= Securities ≠ subject to AMLA	≠ Securities = means of payment under AMLA[3]
ICO of utility tokens[4]		≠ Securities, if exclusively a functioning utility token = Securities, if also or only investment function ≠ means of payment under AMLA if accessory
ICO of asset tokens[4]		= Securities ≠ means of payment under AMLA

Figure 3. Key factors for token classification. © FINMA

60 FINMA, Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs), 16.2.2018.

61 As of May 2019. See p7, ECB Crypto-Assets Task Force.

62 As of October 2018. See CGMF, cryptoassets and crowdfunding, p13.

63 ESMA report distinguishes between payment, investment and utility token, although this distinction does not cover everything and can be hybrid. See p19 ESMA Crypto-Assets.

64 See FINMA Guidelines p4.

65 Standardised instruments suitable for mass trading, i.e. offered for sale publicly in the same structure and denomination, or they are placed with 20 or more clients under identical conditions, as defined in art. 2(b) of the Financial Market Infrastructure Act (FMIA) of 19.6.2015 and art. 2(1) FMIO of 25.11.2015. See FINMA Guidelines p4.

66 See FINMA Guidelines, p5.

entitlement to dividends or interest payments[67]. In terms of their economic function, the tokens are analogous to equities, bonds or derivatives and as such are securities.

FINMA has further clarified that the individual token classifications are not mutually exclusive and tokens may take a hybrid form. In these cases, the requirements are cumulative. Tokens as securities are 'Financial Asset'[68], and the resulting account balance and income fall within the definition of CRS financial information for exchange purposes.

3.3 The concept of 'wallet'

In Blockchain, a wallet is a software that allows cryptographic tokens to be managed via an interface[69]. In its function, a wallet may be described as virtual currency holding accounts, effectively serving as a bank current account on which fiat money can be deposited, stored, and transferred. A cryptographic key pair is needed to carry out transactions: i) a public key (PUK) is an address that serves like an account number, ii) a private key (PIK) serves like a PIN to give full access to the PUK, and the only data in the holder's immediate exclusive possession. If the PIK is lost, the power of disposal over the cryptoassets is also lost. Like a bank account, the PIK must be protected to safely store the assets. Wallets can be differently designed:

– custody wallet providers often manage the key pairs, in particular clients' PIK. It is just a matter of inputing the password into the wallet app;

– decentralised wallet applications are open source projects, often in the form of freewares, that can be not assigned to individual provider companies. Such wallets are referred to as non-custodial wallets, private wallets or self-hosted wallets as they allow users to manage their own key pairs. Proving you own the address is done with a PIK. The developer usually has no knowledge or access to the app users' generated key pairs[70].

67 FINMA publishes ICO guidelines, 16.2.2018 (FINMA portal, last visit 10.6.2019).
68 See Standard for AEoI, Section VIII, A(7).
69 See CGMF, p16.
70 See CGMF, Index.

A study by the University of Cambridge[71] estimated the wallet market in 2016 dto almost 35 million of wallets from 8.2 million in 2013. About 80% of the wallet providers are domiciled either in North America or Europe, whereas only 60% of the users also come from these regions. About 73% of the wallets do not control PIKs, 12% of wallets have an access determined by the user with the PIK, and 15% are custodian wallets. The distinction between wallets and trading platforms has blurred with 50% of the wallets allegedly providing an exchange functionality too (whose activity is generally licence).

3.4 AEoI/CRS: Issues associated with cryptoassets

Cryptoassets challenge traditional financial reporting and accounting boundaries with limited industry guidance. Cryptousers are identified not by names or account numbers but by cryptographic addresses that can be created at any time, by anyone, anywhere[72]. They present features that may pose various issues with regard to CRS obligations, several of which are linked to its very nature, and require further risk analyses: A. Blockchain semi-anonymous and decentralised design; B. data availability and accuracy on Blockchain; C. financial institutions for CRS purposes; D. regulation misuse and misdesign.

A. Semi-anonymous and decentralised design

A wallet, easily set up and free of charge thanks to numerous available programmes, is all what is needed to process crypto transactions. Like a bank account, the walletholder simply orders a transfer to another address of the same type using his PIK or discloses his public address to another user who wishes to debit the wallet. The decentralised design coupled with the distributed consensus, the automated mechanism via smart contracts[73] as well as the asymmetric encryption[74] were developed to secure transactions and guarantee the anonymity. Yet, transactions are visible to all users of this cryptocurrency and can be traced as the system allows the identification of all transactions that originate from or are directed to a specific address. However, the actual

---

71 See CGMF, p16 with reference to Hileman/Rauchs, 2017 Global Cryptocurrency Benchmarking Study, Cambridge Centre for Alternative Finance, University of Cambridge.

72 See Institutionalisation of cryptoassets, Introduction.

73 Smart contracts can automate transaction handling, e.g. move digital assets or function like 'contracts' according to pre-specified rules by writing up the code. As opposed to passive records like databases or excel sheets.

74 Key pair, i.e. the public and the private keys.

identity of the person associated with the wallet remains unknown to the other users[75]. Without physical constraint, enormous cryptocurrency sums can be moved from one account to another within seconds without knowing who is carrying out the transactions. By granting a third-party access to one's wallet, a walletholder can decide to pass on the private key completely undisclosed as if he was passing cash from hand to hand. The unnamed and dispersed design is inherent in the technology and provides the semi-anonymity of transactions, which is exacerbated by the speed and mobility of the system.

B. Data availability and accuracy

In addition to the semi-anonymity feature, a large portion of crypto transactions is carried out directly without a financial intermediary, thus beyond any control, and often without it being possible to determine from which country the transactions were ordered because of the anonymity surrounding wallets[76]. Regulated entities and authorities have hence no data to rely on. Only when cryptoassets are bought or sold for fiat money can the identity of BOs involved be established. However, exchange offices that carry out such transactions on behalf of their customers[77] have no means of verifying the identity of the recipient wallet BOs. Even more, most cryptocurrency exchanges are unable to provide accurate reporting to their users. A striking example is Coinbase, a global digital asset exchange and wallet service company that boasts more than 25 million users on its platform and as such is one of the prominent players in the crypto market. Users can send cryptocurrencies to wallet addresses from or to Coinbase's network at any time. However, Coinbase has no possible way of knowing how, when, where, or at what cost that sent-in cryptocurrency was acquired[78]. This means that anytime cryptoassets are moved off of Coinbase or into Coinbase from another location, Coinbase cannot provide with accurate (historical) information on that cryptocurrency. This means that millions of cryptocurrency users cannot rely on their exchanges to provide them with accurate financial reports and may face problematic uncertainties in tax compliance to the authorities. These issues are inherent in the technology as well. Companies and states have been developing measures and tools to track and aggregate the data.

---

75 See CGMF, p19.
76 See CGMF, p26.
77 See CGMF, p4.
78 Coinbase, 2019 crypto tax guide, Crypto and bitcoin taxes in the US, Updated 24.1.2019.

C. Financial institutions for CRS purposes

CRS is geared toward FIs that are assigned the reporting obligations as well as the due diligence processes. Providing requirements are met, a FI qualifies as a Reporting Financial Institution in a participating jurisdiction when it is *not* a Non-Reporting Financial Insitution[79]. Reportable Accounts in participating jurisdictions are identified financial accounts pursuant to domestic due diligence rules consistent with CRS. Account numbers, or functional equivalent in the absence of an account number, must be exchanged. Hence, the reporting duty lies on FIs that "maintain" reportable accounts and "identify" reportable persons[80]. Yet, CRS provides for an exhaustive list of Non-Reporting Financial Institutions[81], that does not comprise crypto service providers. Similarly, wallets do not meet the definition of Excluded Accounts[82].

In actual fact, companies that offer non-custodian wallets and decentralised trading platforms do not intervene at any time in their users' transactions and therefore do not carry out any financial intermediary activity. These operations are therefore decentralised, dematerialised and disintermediated. They do not know who are the users trading and usually do not record information on anyone. Given the nature of a wallet, it is questionable as to whether a wallet can meet the definition of a 'Reportable Account'. The *wallet* does not actually exist nor store assets. When a wallet displays how many Bitcoins (or most other tokens) are 'deposited' inside it, the wallet software is not counting up a pile of Bitcoins in some account. Instead, it is scanning Blockchain with the user public address as the recipient, i.e. looking through a series of transaction receipts generated everytime someone sent Bitcoins[83]. Nevertheless, if the monies are not in the cryptouser's immediate possession, the exclusive control exercised by the walletholder through its PIK/PUK pair should be enough to qualify the cryptounits as being part of his assets.

For CRS limit exchanges to 'financial account information', cryptoassets will be covered only if each country so decides by considering that they are financial accounts[84]. Meanwhile, governments are trying to extend the scope of FI

---

79 See Standard for AEoI, Part II, Model MCAA, section 1 Definitions.
80 See Standard for AEoI, Part II, Model MCAA, section 1 Definitions.
81 See Standard for AEoI, CRS, section VIII Defined Terms, B.
82 See Standard for AEoI, CRS, section VIII Defined Terms, C(17).
83 Making Sense of Crypto Token Types, skalex.io/crypto-token-types, last visit 28.7.2019.
84 p15, Andres Knobel, Reporting taxation: Analysing loopholes in the EU's automatic exchange of information and how to close them, 15.10.2018.

by reaching the definition to those entities that stand at the intersection between cryptousers and the regulated world, the so-called virtual asset service providers. By doing so, crypto businesses will have to establish due diligence programs similar to those of traditional FIs (e.g. client onboarding processes).

D. Regulation misuse and misdesign

Specific rules apply for financial operations for transparency and investor protection purposes, such as disclosure requirements for legal entities (e.g. establishing BO) or the obligation of elaborated documentation for the distribution of financial instruments[85]. In Switzerland, if the tokens qualify as equity or debt instruments, a token-issuing entity may be required to draw up a prospectus. In practice, the obligation to publish a prospectus can often be avoided during the token issuance[86]. In cases where the tokens to be issued are intended to create cryptographic shares, it is yet to be determined whether a shareholder position (and the corresponding shareholder registry) can be established in this way[87]. Likewise, CRS requirements allow a minimum holding threshold for pre-Existing Accounts[88]. Wallet provider programs automatically generate several addresses for the same wallet. Hence, a user can own several wallets and use a different one for each transaction. By splitting holdings of cryptoassets into a great many wallets, the cryptoholder can keep every account under the threshold that would trigger a reporting obligation.

At present, legal definitions of the various cryptocomponents and the tax treatment of cryptoassets remain limited and vary greatly among countries' tax and legal systems. This situation generates tax and law uncertainties[89] for both the users and the industry. The lack of clear regulatory guidance in certain areas is impacting the ability of the industry to implement appropriate sets of control and processes. These issues reflect in the misuse or the misdesign of existing

---

85 Prospectus Directive (PD) 2003/71/EC as amended, Prospectus Regulation (PR) 2017/1129/EU. See p21 ESMA Crypto-Assets.

86 See Virtual Currency Regulation - Switzerland and p23 ESMA Crypto-Assets.

87 See SIF consultation. In March 2019, Alethena was the first company to successfully tokenise its entire share capital on the Ethereum blockchain. By signing up in the company's digital Share Register, the shareholders hold tokenised shares endowed with claimable rights (dividend and voting rights). Fintechnews, Tokenized Equity: A Revolution for Traditional and New Capital Markets, 14.12.2018.

88 Pre-existing lower-value Accounts: Individual up to CHF 1'000'000, Entity up to CHF 250'000. Reserved are distinctions as regards passive or active non-financial entities.

89 Jonathan Schwarz, Tax certainty: Cure the disease not the symptom, Kluwer International Tax Blog, 28.8.2018.

rules to the cryptoworld and where the set of data required by CRS may be circumvented thanks features inherent in the underlying technology.

3.5 Implementing CRS for Cryptoassets

The EU had a framework in place to govern the use of e-money before the invention of Bitcoin, which has been adaptable to some extent to fit cryptocurrencies. However, under the current state of laws, there is limited scope for public authorities to intervene, a situation further complicated by the lack of governance and the distributed architecture of cryptoassets. The cross-border dimension defies the effectiveness of fragmented government interventions at the national level. There are a number of potential approaches that authorities could take when it comes to the regulation of cryptoassets: A) Cryptocurrency service providers may act as upstream regulators by ensuring that KYC/AML rules are complied with[90]; B) CRS reporting assignment to tax authority shall rest on both FIs and cryptoholders; C) Governments may selectively regulate the industry, impose limitations or provide supporting mechanisms to incentivise users and enforce compliance. The KYC/AML approach and the shift of reporting duty from FIs to cryptoholders will be detailed in the following sections while government measures will be addressed in chapter IV.

A. KYC and AML regulations

The global AEoI Model is drafted with respect to financial account information that need to be reported by FIs. Crypto businesses should look to establish due diligence programs similar to those of traditional FIs. A KYC program primarily focuses on verifying client identities where AML requirements tackle transaction compliance. However, as crypto transactions are usually transnational and run through service companies registered in a great many countries, the lack of international standards in due diligence obligations among all financial intermediaries inevitably reflects in the limited effectiveness of these precautionary measures. Hence, despite their willingness to cooperate with the authorities, FIs are not yet in a position to provide data on the identity of their clients or the origin of tokens which they trade with.

---

90 Some of the existing exchanges, such as Coinbase, already enforce these regulations. Andrew Norry, An In-depth look at Bitcoin laws & future regulation, Blockonomi, 2.7. 2018.

a) EU 5th Anti-Money Laundering Directive

In late 2015, following the Paris terrorist attacks, EU ministers called for a "strengthening of controls" around cryptoassets, discovering their potential use in terrorist fundraising[91] and money laundering. The European Parliament (EP) overwhelmingly backed changes to AML/CTF legislation in order to impose new regulations on crypto exchanges and custodians operating in Europe. On 30 May 2018, for purposes of identifying users of virtual currencies, the EP and the CEU adopted an amendment to the 4th Anti-Money Laundering Directive[92], known as the 5th AMLD[93], which extends the scope of the directive to custodian wallet providers and to platforms for exchanging virtual and fiat currencies. These categories of business will become "obliged entities" under the new AML/CTF rules and will be held to the same standards as traditional FIs in order to ensure that virtual currencies cannot be used to "obfuscate"[94] the trail of money. The 5th AMLD entered into force on 9 July 2018 and MS have by 10 January 2020 to transpose its provisions into their national legislation. The Directive marks a key development in cryptocurrency regulations and will effectively bring the world's second largest economy in line with cryptocurrency measures introduced in the USA a few years earlier. The Directive defines 'virtual currencies'[95] as "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." A 'custodian wallet provider' is "an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies"[96].

The primary focus of the 5th AMLD is to increases transparency of virtual currency transactions by establishing national centralised registers of companies and other legal entities, and their ultimate BOs. International cooperation

---

91 Thereafter 'CTF', counter-terrorism financing.

92 Directive 2015/849/EU on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and Directives 2009/138/EC and 2013/36/EU.

93 Directive 2018/843/EU.

94 Section I Background (4), FATF (2019), Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris. Thomas Wahl, 5th Anti-Money Laundering Directive, Eucrim, 20.10.2018.

95 Art. 1(2)(d) of the 5th AMLD, that should not be confused with e-money nor in-games currencies (recital (1) of the 5th AMLD).

96 Art. 1(2)(d) of the 5th AMLD.

shall be enhanced so that a centralised automated mechanism for payment and bank accounts as well as national corporate ownership registers[97] can be interconnected[98] and accessible to all MS for identification and exchange purposes. Information on BOs of trusts and similar arrangements is clarified[99] and for the first time available to the general public, but only to those who show a legitimate interest[100]. MS may retain the right to provide broader access to information in accordance with their national law. Towards their national AML authorities, the obliged entities have to: i) register; ii) enhance customer due diligence measures; iii) increase transparency and collect data on BOs and third parties, and give access to BO registers[101]; iv) report suspicious transactions; and v) countinously monitor virtual currencies transactions.

As the EC has recognised, including crypto exchange platforms and custody wallet providers as obliged entities "does not entirely address the issue of anonymity attached to virtual currency transactions, as a large part of the virtual currency environment w[ould] remain anonymous because users can also transact without these providers." The 5th AMLD proposes therefore that MS create central databases consisting of virtual currency users' identities and wallet addresses, in addition to those using exchange platforms and wallet custodians, and directs MS to authorise National Financial Intelligence Units (FIUs) to access these databases. FIUs will be able to obtain information allowing them to link virtual currency addresses to the identity of cryptoowners regardless of whether these obliged entities have filed suspicious transaction reports[102]. Companies dealing with customers from high risk third countries will be required to apply enhanced safeguards, specifically focused on addressing the risk posed by deficiencies in those countries' AML protections,

---

97 Electronic data retrieval systems to identify natural or legal persons holding or controling payment accounts, bank accounts, and safe-deposit boxes; implementation by 10 September 2020. Art. 1(19) of the 5th AMLD resp. regulation (EU) 910/2014.

98 Via the "European Central Platform", that must be completed by March 10, 2021. Art. 1(15)(g) and (42) of the 5th AMLD, Directive (EU) 2017/1132 of 14 June 2017.

99 It shall include all the persons listed under Art. 3(6)(b) of the 4th AMLD respectively Standard for AEoI, B. CRS, Section VII (D, 6), i.e. the settlor(s), the trustee(s), the protector(s) (if any), the beneficiaries (or where the individuals benefiting from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates), and any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means.

100 Art. 1(16)(d) of the 5th AMLD. e.g. obliged entities in the context of their due diligence measures, investigative journalists or NGO.

101 At MS level through central registries of bank and payment accountholders.

102 Within FIUs' obligations under the 5th AMLD. Art. 1(15)(c) of the 5th AMLD.

where though many exchange platforms and custody wallet providers are thought to be located. The 5th AMLD also puts forward a mechanism of self-declaration forms to be submitted by cryptousers. The EC is giving consideration to further harmonising the AML/CTF rulebook by upgrading AMLD into a Regulation[103], which in contrast to a directive is binding on MS. This transmformation would have the potential of setting a harmonised, directly applicable regulatory AML framework.

b) FATF Recommendations Update

In 2014, FATF has emphasised the potential risks of virtual currencies and published a guidance for a risk-based approach to assessing dangers relating to the Blockchain ecosystem. It addressed the role of hosted wallet providers (2017) and introduced relevant definitions[104] (2018). In june 2019, FATF developed recommendations[105] and adopted an updated version of its guidance now entitled "Virtual Assets and Virtual Asset Service Providers"[106]. Where the EU 5th AMLD introduces regulation for crypto-to-fiat exchanges and custodian wallet providers, FATF 2019 Guidance details how its Recommendations should apply to virtual assets (VA), VA financial activities and Virtual Asset Service Providers (VASPs). VA is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. VASP is any natural or legal person who has a business conducts for or on behalf of another person in one or more of the five categories of activity or operation: i) exchange between VAs and fiat currencies; ii) exchange between one or more forms of VAs; iii) transfer of VAs; iv) safekeeping and/or administration of VAs or instruments enabling control over VAs; and v) participation in and provision of financial services related to an issuer's offer and/or sale of a VA[107]. Thus, FATF target users in a business context or for commercial purposes and excludes situations where cryptocurrencies are merely used to buy goods and services. Countries are recommended to apply

---

103 European Commision, Communication from the Commission to the European Parliament and the Council, Towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework, 24.7.2019 COM(2019) 360 final.

104 See Section I Background (5), FATF (2019).

105 FATF (2012-2019), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France

106 FATF (2019), Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris.

107 See Section II (35), FATF (2019). VASPs include VA exchanges and transfer services; some VA wallet providers; providers of financial services relating to the issuance, offer, or sale of VA (e.g. ICO); and other possible business models.

a risk-based AML/CFT approach to those assets, regulate, monitor, and supervise VASPs, and facilitate information sharing between authorities. In order to enforce a level playing field with traditional FIs, VASPs must be licensed and perform standard AML/CFT processes such as customer due diligence, PEP[108] screening, reporting, and record keeping. Additionally, countries are urged to identify and sanction any VASP that conducts business without being properly registered.

Recommendation 16 introduced a preventive measure, referred as the 'Travel Rule[109]', that gave rise to passionate argument in the blockchain sphere. VASPs must collect and share information about customers transactions of more than USD/EUR 1'000[110], including those of the fund recipients. While the Travel Rule makes sense when all financial transactions are sent through intermediaries, the main stumbling block resides in that VA transactions can take place not just on crypto exchanges or similar services, but also through peer-to-peer (P2P), person to machine, via smart contracts, etc. Notwhithstanding an onerous implementation of systems to collect and transmit data, people in the industry wonder about how these recommendations will apply to crypto and their effects. Many experts in the field fear that it may drive cryptousers, and therefore criminal users, underground[111] and migrate to decentralised exchanges (DEX) to avoid government oversight. FATF standards provide indeed for exceptions for payments involving unregulated wallet providers[112]. In a real DEX, exchanges take place directly between users in a P2P way[113], rendering it technically impossible to impose KYC/AML procedures on such exchanges. Moreover, so as to limit any government interference DEXs allow users to retain full and exclusive possession of their private keys.

While they may be called Recommendations, FATF includes all the key financial systems that will implement them as binding international law[114]. The G20

---

108 Politically Exposed Persons.

109 Paragraph 7(b) Recommandation 16, FATF (2012-2019).

110 Countries may adopt a *de minimis* threshold for wire transfers (less than USD/EUR 1'000). Para. 5 and 6 INR16, FATF (2012-2019).

111 Lukas Hofer, FATF Publishes New Crypto Guidelines - Threat or Opportunity? 24.6.2019.

112 FINMA Guidance 02/2019, Payments on the blockchain, 26.8.2019.

113 Marco Cavicchioli, FATF recommendations for crypto could favour DEXs, The Cryptonomist, 24.6.2019.

114 The US Treasury Secretary Steven Mnuchin stated: "The [FATF] Interpretive Note adopted this week includes virtual asset standards that are binding to all countries. […] This will enforce a level playing field for virtual asset service providers, including cryptocurrency

already reaffirmed it would align with the FATF standards and MS have been eager to endorse the Recommendations. Countries have 12 months to adopt the guidelines with a review set for June 2020. FATF's scope is broader than that of 5th AMLD. With this in mind, some MS are considering a extended approach in their national legislation[115], such as regulations to be applied to all digital assets and not just cryptocurrencies, to exchanges virtual-to-virtual and virtual-to-fiat transactions and interactions involving VAs[116], and for an extra-UE territorial scope to those providing services to people in the UE, even where the provider is based outside the UE[117]. Countries are required to make not only companies, but also their directors and senior management subject to sanctions for failure to comply with the Recommendations and other AML/CFT requirements.

c) Exchange offices and trading platforms

The exchange activity for cryptoassets is the most significant market with numerous companies operating in this sector. Exchanges are the primary entry point by which cryptocurrency traders and customers interact. As a result, many jurisdictions are focusing on the regulation of exchanges and thereby ensuring that they apply customers KYC processes at the point of registration or time of transaction. 'Gatekeeping' service providers[118] must have accounts verified or an upper limit to which accounts remain unverified. Activity carried out by centralised service providers relies on a set-up that similar to that of traditional FI business, hence a similar legal framework could be used to regulate the activities of centralised gatekeepers. In Switzerland, exchanging fiat-to-cryptocurrencies or two different tokens constitutes a financial intermediation activity subject to the Anti-Money Laundering Act (AMLA)[119].

A distinction can be generally made between online exchange offices and trading platforms. If a service provider offers the exchange services directly in a bipartite relationship, i.e. acts as an exchanging counterparty, such activity qualifies as money exchange under AMLO[120]. Centralised and decentralised

providers, and traditional financial institutions." Gordon/Wong, Crypto exchanges have 12 months to implement FATF anti-money laundering standards, 4.7.2019.

115 See FATF - Threat or Opportunity?

116 See Section I (5), FATF (2019).

117 See Crypto exchanges have 12 months.

118 See p. 29, ECB Crypto-Assets Task Force.

119 Swiss Federal Act on Combating Money Laundering and Terrorist Financing, 10.10.1997.

120 See CGMF, p17. Art. 51(1)(a) Anti-Money Laundering Ordinance (AMLO) for entities that are subject to FINMA supervision or the relevant regulations of the SROs.

trading platforms serve in a tripartite relationship in that they assume an intermediary function and maintain a customary order book. In centralised platforms, users trade directly on the platform (off-chain). Users either deposits their tokens with the platform or use a wallet to which the platform has access[121]. Centralised platforms as "money transmitters[122]" qualify as financial intermediary and is subject to AMLA. Decentralised platforms do not control the clients' wallet. The orders take place directly on Blockchain between the users[123] and can be settled using a smart contract. Even though a transfer of assets ultimately takes place, decentralised platforms do not qualify as a financial intermediary service provider within the meaning of AMLA.

Exchange offices are able to provide with information on the BO identity[124] when cryptocurrencies are being bought or sold for fiat money. Major exchanges have undertaken the collection of KYC data and are now an important source of information for the identification of addresses for certain cryptoassets[125]. However, there will continue to remain a sizable percentage of addresses that have no available KYC data[126]. As well, depending on the qualification of FIs pursuant to CRS, reporting assignment on FIs differ greatly. This point is beyond the scope of the present paper and will not be treated.

d) Data tracing and aggregating

Common belief falsely assumes that crypto is so anonymous that identification is not enforceable. Most cryptocurrencies are not anonymous, but rather pseudonymous: chain analysis is used to check whether the client's wallet actually contains the bitcoins he wants to sell. However, this offers only very limited assistance since chain analysis is possible only for certain traceable cryptocurrencies or the trail can be definitely interrupted with some techniques. Even if the assets concerned can be traced using chain analysis, this analysis does not provide any data about the wallet BOs involved in the transactions. Certain chain analysis programs, however, can compare the transactions carried out between different wallets relatively accurately, making it

121 i.e that hold power of disposal over the assets, similar to storage services.
122 Art. 4(2) AMLO. See CGMF, p17.
123 On a P2P basis, among possibly unauthenticated users. See CGMF, p18.
124 See CGMF, p29.
125 See Institutionalisation of cryptoassets, "Introduction".
126 Cf above, Cambridge report, The concept of wallet.

likely to determine whether their BO is always the same. This identification seems to be possible with information provided by financial intermediaries[127].

Governments focus on cooperation with crypto exchanges, programs for screening user data and government regulations. Australia is cracking down on cryptoinvestors by using a combination of data matching and "100-point identification checks"[128]. The US Securities and Exchange Commission (SEC) is looking for a big data tool to monitor blockchains[129] while Nasdaq, North America's largest electronic exchange, reports that seven crypto exchanges are already using its monitoring technology to detect illegal market activity[130]. Collection records[131] from designated service providers have started in Australia, the UK, Belgium, Austria and Denmark[132]. A tax calculator application, known as Recap, has been launched with the support of the UK Government, in order to help cryptoholders to calculate their tax positions[133]. By linking wallet addresses and exchange accounts, the platform then extracts transaction data, values, and prices. Delaware[134] is testing tamper-proof company registry, which would make KYC regulations easier to comply with.

Businesses in the crypto sphere and in other industries, in particular those based on a digital economy model, also have interest in collecting data. In April 2018, Amazon received a patent for a "streaming data marketplace" that would permit the combination of multiple data sources, thereby enabling the real-time tracking of cryptocurrency payments and the users involved[135]. This technology could potentially be offered to governments, who would be able to correlate crypto addresses to official IDs and/or IP (Internet Protocol) addresses of the transactions to countries of origin. In January 2019, four South

---

127 See CGMF, Section 3.2.2.

128 Molly Jane Zuckermann, Autralia: Experts say tax office on 'Warpath' against crypto investors, Coin Telegraph, 15.6.2018.

129 Yogita Khatri, US SEC seeking big data tool for major blockchains, CoinDesk, 4.2.2019.

130 Michael del Castillo, Nasdaq is now working with 7 cryptocurrency exchanges, Forbes, 30.1.2019.

131 Australian Taxation Office, Tax treatment of crypto-currencies in Australia, ato.gov.au.

132 American Crypto Association, Denmark's Tax Agency to collect information about Bitcoin traders, 15.1.2019.

133 Paddy Baker, The UK is quietlyp preparing to chase unpaid crypto taxes, Crypto Briefing, 8.8.2019.

134 Carlos Santiso, Can blockchain help in the fight against corruption? World Economic Forum, 12.3.2018.

135 Simon Chandler, Government tracking of crypto is growing, but there are ways to avoid it, Coin Telegraph, 7.10.2018.

Korean exchanges[136] formed a team with the aim to create a shared database and to transmit real-time data among each other. Given the arrival of such tracing and screening data technologies, it is only a matter of time before transactions involving non-privacy cryptocurrency such as Bitcoin and Ethereum will be systematically de-anonymised.

Tracing account ownership enables to address another hurdle inherent in the technology. Pursuant to CRS, a reporting FI is required to aggregate all financial accounts maintained by that FI[137] for purposes of determining the aggregate balance of financial accounts held by a reportable person. Aggregating wallets back to single cryptoholders would prevent these holders from taking advantage of the minimum threshold feature for pre-Existing Accounts as allowed by CRS or for relevant Financial Account under mandatory reporting regimes[138]. Finish P2P trading platform LocalBitcoins has implemented AML/KYC processes for 'high volume' accountholders[139] In line with the country's effort to upgrade its laws with the EU 5th AMLD. However, cryptousers and VASP may face poor recording keeping or missing data of transactions from the very beginning of client's cryptocurrency usage because of either the absence of appropriate infrastructure or unclear/inexistent rules. In addition, the users may have transactions separate from exchanges, such as P2P trading, transferring to a wallet or investing in an ICO. Hence, it is often difficult for the intermediary to correctly establish account balances and income. Cryptocurrency softwares can be used to automatically associate data to crypto transactions. The tools import historical trade data from cryptocurrency exchanges like Coinbase to then generate the reports that contain the necessary information. Not all softwares are built equally and report reconciliation from a great many operating exchanges can be tedious. If the tools do not support one of these platforms, getting the historical data into the program can be incredibly complex, resulting in data inaccuracies. Last but not least, many platforms also limit the amount of data that can actually be imported[140].

---

136 Nicola Filzmoser, Governments track the crypto space, Blockpit, 13.3.2019.

137 See Standard for AEoI, Section VII, C.

138 See below Reporting assignement on the taxpayer. Promoters must disclose relevant Financial Account value or balance USD 1'000'000 or above in CRS Avoidance Arrangements. OECD (2018), Mandatory Disclosure Rules for Addressing CRS Avoidance Arrangements and Opaque Offshore Structures, Questions and Answers.

139 Coin Path, Localbitcoins warns over 'major changes' for users in AML/KYC crackdown, 11.2.2019.

140 Kemmerer/Yip/Azran, Common Issues Encountered in Crypto Tax Compliance, News Bloomberg Tax, 12.6.2019.

At multinational level, FATF has proposed enhanced due diligence measures with regard to high risk countries such as corroborating the customer's identity through a national identity number or through information from third-party databases or other sources, as well as tracing the customer's IP address, geo-location data, wallet addresses, and transaction hashes. In addition, the MCAATM and the spontaneous exchange of information regime can complete the set of measures applied by countries[141]. Any information pertaining to foreign citizens and businesses' identity and transaction data will reportedly be passed over to their respective countries' tax authorities[142].

B. Reporting assignement on the taxpayer

In practice, CRS function has revealed various loopholes such as non-reporting jurisdictions and low-tax jurisdictions that provide golden passports and can be used to disguise a taxpayer's residency, or intermediate companies can hide the ultimate BO in a reporting chain[143]. In order to provide tax administrations with information on arrangements that (purport to) circumvent the CRS and on structures that disguise the BOs of assets held offshore, the OECD Model Mandatory Disclosure Rules for CRS Avoidance Arrangements and Opaque Offshore Structures (MDR) were approved by the Committee of Fiscal Affairs on 8 March 2018[144]. The EU has added further impetus on 25 May 2018 to enhanced international tax transparency with the enactement of DAC6[145], a directive on mandatory automatic exchange of information in the field of taxation in relation to reportable cross-border arrangements. DAC6 was built on the OECD BEPS project (Action 12 mandatory disclosure rules for aggressive tax planning schemes) and drafted to insulate the CRS against new avoidance schemes designed to undermine its requirements. At their core, both directives impose the mandatory reporting of cross-border arrangements that are indicative of aggressive tax planning schemes affecting at least one MS. The disclosure requirements will have to be followed by 'intermediaries' and, in some instances, the taxpayers. There are essentially two strands:

---

141 See Autralia: 'Warpath' against crypto investors. Crypto Season, Denmark targets 2,700 Bitcoin taders for tax payments after tip-off from Finland, 12.12.2018.

142 Molly Jane Zuckermann, Belgian tax authoritiy to search for taxpayers using foreign crypto exchanges, Coin Telegraph, 4.3.2018. See Denmark's Tax Agency to Collect Information.

143 See Executive Summary, Analysing loopholes in the EU.

144 See Standard for AEoI, B. CRS, Section IX: Effective Implementation.

145 Amendment to Council Directive 2011/16/EU.

– MDR took effect from March 2018. OECD MS have discretion around implementing these rules;

– DAC6 mandatory rules aim at a much wider range of activities than MDR. EU MS including Cyprus will transpose DAC6 into national law by 31 December 2019 and apply the provisions as from 1 July 2020.

The purpose of MDR is to provide tax administrations with information on CRS Avoidance Arrangements and Opaque Offshore Structures and bolster the overall integrity of the CRS. The implementation of DAC6 aims to provide MS with information to enable them to promptly react against harmful tax practices and to close CRS loopholes. Because most of those tax schemes have cross-border character, DAC6 widened the type of data to be automatically exchanged among all affected countries. Mandatory disclosure regimes are expected to act as an *ex ante* mechanism to deter taxpayers from implementing abusive tax schemes[146]. For the scope of DAC6 is broader thant MDR, MS could use the work of the MDR as "a source of illustration or interpretation, in order to ensure consistency of application across Member States[147]". In line with DAC6's statement and although both directives differ in some provisions, DAC6 and MDR will be equally addressed in the following paragraphes as regards the CRS parts.

a) Mandatory information reporting regimes

DAC6 provides for general rules on who must report and when, and what information[148] must be reported. One key point of DAC6 is the absence of definition of aggressive tax planning. For a cross-border transaction to be reportable, it must contain one of the general or specific 'hallmarks' set out in Annex IV of the directive. 'Hallmark' features deemed possible indicators of tax abuse lead either to a 'main benefit test', which will be met if obtaining a tax

---

146 Preamble #7 DAC6. Marina Serrat, Tax EU Directive 2018/822: Opening Doors for a Common Cooperative Compliance System on Taxation? 8 August 2018, Global Tax Blog Gov. (globtaxgov.weblog.leidenuniv.nl/2018/08/09/eu-directive-2018-822-opening-doors-for-a-common-cooperative-compliance-system-on-taxation, last visit 15 August 2019).

147 Preamble #13, Council Directive 2018/822/EU (DAC6) of 25 May 2018, amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation in relation to reportable cross-border arrangements.

148 Although each MS will impose DAC6 into national legislation, the information that will need to be reported is the following: identification of all intermediaries and relevant taxpayers (names, dates and place of birth, tax residence, TIN, and, where applicable, associated enterprises, details of the arrangement (value, summary, date, description of business activities), details of the hallmark(s), details of the relevant national law, etc.

advantage constitutes the main benefit[149] (or one of the main benefits) of the arrangement, or refer to arrangements which are perceived to circumvent designated tax anti-avoidance rules such as CRS or transfer pricing rules. These include where the arrangement seeks to take advantage of the absence of such rules[150] as well as those to obscure the real BO of the structure or assets. As a result, even if the arrangements are not purely tax-driven, the parties involved will still need to consider DAC6 disclosure and file information that is within their knowledge, possession or control on reportable cross-border arrangements. There is thus no safe harbour for *bona fide* arrangements having an underlying commercial, technical or financial purpose. This is a subjective standard that looks at whether entity classification, documentation, due diligence and reporting have the effect of undermining the objectives of CRS.

CRS Avoidance Arrangements and Opaque Offshore Structures are arrangements that are designed to circumvent, or are marketed as, or have the effect of, circumventing the CRS (as implemented in relevant national laws). An 'intermediary'[151] is an individual or company that designs, markets, organises or makes available for implementation or manages the implementation of a reportable cross-border arrangement in light of its CRS treatment or for preventing the identification of the BO for a relevant taxpayer. The directive requires an intermediary of an arrangement that resembles an Arrangement or Structure to: 1) disclose factual descriptions of the Arrangement or Structure; 2) identify those involved in the Arrangement or Structure, including other intermediaries; and 3) establish the jurisdiction(s) in which the Arrangement or Structure is available to implement. Disclosure must take place within 30 days after the intermediary makes the Arrangement or Structure available to implement or after the intermediary provides what are considered "Relevant Services[152]". For the disclosure obligation to be effective, intermediaries need to have a sufficient nexus with the reporting jurisdictions (e.g. residence, branch, incorporation). DAC6 is particularly relevant for lawyers, in-house counsel, accountants and financial advisers who, or through others, provide aid, assistance or advice in any of the above matters, and knows or could reasonably be expected to know[153] (having regard to the relevant facts and circumstances)

149 Cf Principal Purpose Test (PPT) of OECD BEPS Project.

150 Daniel Dzenkowski, DAC6 Hallmark D requires a different approach, PWC, 30 July 2019.

151 Art. 3(21) DAC6.

152 i.e. responsible for or providing assistance or advice with respect to the design, marketing, implementation, or organisation of that arrangement or structure. Rule 1.4(k) MDR, rule 2.6(c) MDR, art. 1(1,b,19) DAC6.

153 Commentary #47 MDR.

that it relates to a reportable cross-border arrangement. The information required to be disclosed includes the intermediaries involved with the design and set-up of such arrangements and the taxpayers using those.

In autumn 2016, the author was invited to a meeting where prospect investors were introduced to the Bitcoin world and guided by a cryptocurrency trader to 'open' a (freeload app) wallet. Does this financial advisor fall within the scope of the directives as an 'intermediary' where he acted towards EU taxpayers as a promoter or service provider of an arrangement "that encouraged their client to enter into an arrangement on the basis that it was not subject to CRS reporting", respectively are these investors in scope of the directives as EU taxpayers where they benefited from the arrangement?[154]

A 'Service Provider' is any person whose knowledge of the Arrangement combined with appropriate level of expertise and understanding enable that person to provide Relevant Services knowing the arrangement lead to such CRS outcomes or when that person knows or can be reasonably expected to know that the arrangement is a CRS Avoidance Arrangement[155]. The definition would capture a Service Provider that works closely with the Promoter in designing or marketing the arrangement as well as a person who assists a Reportable Taxpayer to enter into an arrangement subject to disclosure. Both Promoters and Service Providers are defined, not by reference to the role or occupation of the person[156], but by the role they play in providing Relevant Services for the arrangement. Pursuant to MDR, the use of an account, product or investment that does not fall within the definition of an CRS reportable account but whose features are substantially similar to reportable accounts[157], or the conversion of a reportable account or money or assets held in a reportable account into an account that is not reportable under CRS[158], constitute CRS Avoidance Arrangements. Under the definition, the mere request to make such an Arrangement makes an individual a "Client[159]" for purposes of MDR. Nonetheless, an intermediary is not required to disclose a Reportable Taxpayer that is a potential user of the arrangement, for example simply because the person attended a presentation or received marketing materials about a CRS Avoidance Arrangement. However, the user's identity must be disclosed by the

154 Commentary #51 MDR.
155 Rule 1.1 MDR, art. 1(1,b,19) DAC6.
156 See Mandatory Disclosure Rules, Questions and Answers.
157 Rule 1.1(a) MDR.
158 Rule 1.1(c) MDR.
159 Rule 1.4(d) MDR.

intermediary, if the intermediary is being notified to implement or requested to provide with Relevant Services in respect of that arrangement[160].

The first reports pursuant to DAC6 must be filled by 31 August 2020 and involve data on reportable transactions undertaken between 25 June 2018 and 1 July 2020; respectively, MDR calls for disclosures related to CRS Avoidance Arrangements entered into between 29 October 2014 and the effective date of the rules (Figure 4). This means that the directives generate a twofold uncertainty: the retrospective element (which means it is already necessary to consider its effect) and the yet to be published legislation under which MS will transpose the directive. This become challenging since each tax jurisdiction has the discretionary right to adopt and implement DAC6 and MDR into national legislation; hence, similar to OECD BEPS Action Plan provisions could differ in some important details between MS based on their specific circumstances leading to an uneven implementation and jurisdictional exchange.

b) Subsidiary reporting obligations

Where no intermediary is involved or required to perform the reporting of the cross-border arrangement; either because the intermediary is outside the scope of the rules or bound by the requirements of professional secrecy[161], a direct disclosure obligation shifts to the relevant taxpayers. In these cases, the reportable taxpayer has to provide all relevant information on the arrangement or structure that is within its knowledge, possession or control. By imposing a subsidiary disclosure obligation onto the taxpayer could prevent the taxpayer from insulating itself from the effect of the rules[162]. Non-resident taxpayers in a MS[163] are not exempt from these rules. To the extent such taxpayers carry on activities in a MS, they may be required to make a disclosure. The penalties for failing to comply will be set by each MS[164]. Weirdly, reporting by a taxpayer is not required where disclosure is limited by domestic protections against self-incrimination[165]. Would a taxpayer, who has implemented an unlawful CRS Avoidance Arrangement, calls for this exception to the disclosure rule – provided the jurisdiction has such a provision against self-incrimination

160 Commentary to Rule 2.3(a, iii) MDR.

161 Only insofar as an information request for the same information could be denied under Art. 26 of the OECD Model Tax Convention and Art. 21 MCAATM. See MDR.

162 Commentary #86 MDR.

163 DAC6 expected consequences will include organisations and individuals in Switzerland and Liechtenstein. See CGMF, pt 4.2.

164 Commentary #89 MDR.

165 Commentary #86 MDR.

– that taxpayer appears to be ‘protected’; however, the taxpayer who has implemented a *legal* CRS Avoidance Arrangement, which presumably would not implicate the protection against self-incrimination, would not be ‘protected’.

The rollout of mandatory disclosure regimes means FIs will have to compile a two-year backlog of transactions in time for the first reports to be exchanged on 31 October 2020 (DAC6) through a centralised database[166]. It is however unlikely that possibly affected crypto service providers such as virtual currency exchange platforms have the required information on reportable transactions undertaken as far as 25 June 2018, either because they do not have a structure in place to collate data, or appropriate legislation were not in place yet. The definition of CRS Avoidance Arrangements is extremely broad and far reaching, likewise DAC6’s very broad scope makes it an almost ‘catch-all approach’[167] to tax planning and cross-border transactions. The subjectivity and broad room for interpretation force FIs, and taxpayers, to think about whether they are part of a scheme that is trying to defeat the CRS.

IV. Developments in selected countries

As of today, there are no unified international regulations that apply to the whole crypto-community. Vulnerabilities often lie at the level of financial intermediaries that carry out crypto transactions, at the point where cryptousers enter and propagate into the regulated financial sector. Countries are finding their own ways to operate against crypto-related criminal cases. Whether through amending the existing regulatory framework, creating a new legal, crypto-specific basis or implementing technological developments to directly track users' data, the response has been hitherto inconsistent and states around the world are constantly developing new measures to track criminal activity.

4.1 Switzerland

Where many other countries have banned or limited the use of cryptocurrencies and relating activities[168], three ICOs out of ten belonged to Swiss

166 Every 3 months Art. 8a (2, 18) DAC6. For MDR, “the OECD is currently working on an exchange of information framework for the new rules”.

167 Josh White, Banks feel the strain of getting ready for DAC6, International Tax Review, 25.1.2019.

168 See Virtual Currency Regulation - Switzerland.

companies. Swiss financial market regulation is principle-based and technology-neutral: it applies to cryptoassets and cover crypto related activities, and ICOs to a large extent[169]. AMLA is built around a pillar: the financial intermediary[170]. In FINMA's view, all types of financial intermediaries[171] that carry out crypto transactions are subject to AMLA; the scope is hence relatively comprehensive by international comparison. AMLA qualifies a financial intermediary anyone who provides payment services or who issues or manages a means of payment. The issuing of payment tokens or utility tokens that encompass any form of payment function constitutes the issuing of a means of payment subject to AMLA[172] insofar as the tokens can be transferred technically on Blockchain, at the time of the ICO or only at a later date. In this respect, financial intermediaries need to follow a range of due diligence steps: requirement to establish the identity of the BO and contracting parties, obligation either to affiliate with a self-regulatory organisation (SRO) or to be directly supervised by FINMA. The accepted funds must be deposited via a financial intermediary who is already subject to AMLA and who exercises on behalf of the organiser the corresponding due diligence requirements. Under current FINMA practice, the regulation applies to the exchange of a crypto-for-fiat currency or crypto-for-crypto currency as well as the offering of services to transfer tokens if the service provider maintains the PIK[173]. The issuance of asset tokens does not qualify as financial intermediation activity pursuant to the AMLA, if such asset tokens qualify as securities and are not issued by a bank, securities dealer or other prudentially supervised entities[174]. In practice, issuers of asset tokens often conduct various KYC and identification measures on a voluntary basis relating to bank's compliance requirements to which the proceeds of the ICO will be transferred. It should be noted that restrictions of US Securities Law are also relevant for Swiss ICOs[175].

---

169 At present, there is no binding legal qualification of tokens notwithstanding FINMA ICO guidelines. SIF, Federal Council initiates consultation on improving framework conditions for blockchain/DLT, 22.3.2019 with reference to Legal framework, Executive Summary.

170 Carlo Lombardini, Les dérives de la lutte contre le blanchiment, Le Temps, 8.9.2019.

171 See point 3.6, letter A and CGMF. Wallet providers have a general identification duty from CHF 0 (art. 3 AMLA), exchange platfeform from CHF 5'000 for (art. 51(1, a) AMLO).

172 Art. 2(3, b) AMLA except case as defined in art. 2(2, a, 3) AMLO. See CGMF p13. FINMA Circ. 11/1 "Financial intermediation under AMLA" margin no. 13 et seq. See FINMA Guidelines, p7.

173 Custody wallet provider. See The concept of 'wallet'.

174 See FINMA Guidelines, p7.

175 See below United States.

On 26 August 2019, FINMA published a supervisory note on the application of certain regulatory requirements relating to payments in the context of cryptoassets. Financial intermediaries shall apply art. 10 AMLO-FINMA[176], also referred to as 'travel rule[177]', that specifies the information to be transmitted by intermediaries when they make transfers. Required information in payment transactions comprise the data relating to the payer and the beneficiary. Such information generally cannot be integrated in the transfer, the transmission can hence occur separately by the means of communication of choice. This requirement is based on FATF INR16. Unlike the FATF standards, art. 10 AMLO-FINMA does not provide for any exception for payments involving unregulated wallet providers[178] (nonetheless, non-custodian wallet providers and certain decentralised trading platforms for cryptobased assets are not subject to AMLA yet[179]). FINMA goes even further stating that as long as a regulated FI is not able to send and receive the required information, such transactions are only permitted from and to external wallets if these belong to one of the FI's own customers, and their ownership of the external wallet must be proven. Transactions between customers of the same institution are permissible while a transfer from or to an external wallet belonging to a third party is only possible if the FI has the background and identity of the third party and the account BO verified[180].

There is currently no specific legislation addressing the regulatory status of miners, the mining of tokens does not trigger a licence requirement[181] while centralised trading platforms require FINMA licences. On 26 August 2019[182], FINMA confirmed that two pure-play blockchain service providers have been granted banking and securities dealers' licences. Parallely, many tax

176 FINMA Ordinance on anti-money laundering (AMLO-FINMA), 3.6.2015. See p2 FINMA Guidance.

177 Jeremy Bacharach, Does Communication 02/19 have a sufficient legal basis? The Center Research Education Agenda, cdbf.ch/1082, 2.9.2019.

178 See p3 FINMA Guidance.

179 The challenges arising in this connection generally have to be addressed internationally within the context of the work of the GAFI. See CGMF, Introduction.

180 Switzerland is participating in the Titaniun project (Tools for the Investigation of Transactions in Underground Markets), a common initiative from several countries under the leadership of Interpol, which aims to develop a tool to improve the transparency of crypto transactions, in particular, a simultaneous analysis of blockchains of different cryptocurrencies in order to break the anonymity of their users. See CGMF, pt 4.2.

181 See Virtual Currency Regulation - Switzerland.

182 FINMA guidance: stringent approach to combating money laundering on the blockchain, Press release, 26.8.2019.

professionnals are of the opinion that the token categories developed by FINMA's ICO Guidelines will also be applicable for tax purposes[183]. Both FTA and the cantonal tax administrations are then expected to soon publish practice guidelines on the taxation of tokens.

4.2 France

French Central Bank considered that cryptoassets are not 'real' money. As a result, under French law, it is impossible to impose a party to accept cryptoassets as payment nor do cryptoassets carry a repayment guarantee at face value in the event of unauthorised payment. As of today, the mining activity is permitted and unregulated notwithstanding specific applicable taxation. Until recently, there was no specific regulations governing cryptoassets, unless they fall within the existing legal framework governing securities offering and trading following Financial Markets Authority's (AMF) token qualification as utility tokens or security tokens. However, this is changing with the adoption on 11 April 2019 of the optional clearance for ICOs subject to AMF approval.

In the last two years, France is trying to step up to the forefront of the blockchain revolution in the EU and works to establish a favourable legal framework for ICOs. Cryptoassets related issues are addressed either i) by extending the scope of existing laws to treat ICOs as public offering of securities, based on an analysis on a case-by-case basis by the AMF depending on the rights and obligations conferred to each cryptoasset (e.g. AML, tax), ii) by proposing *ad hoc* regime adapted to ICOs (e.g. decree of 8 December 2017 related to the registration of unlisted securities on Blockchain), or iii) by promoting best practices without changing existing law. However, the blockchain legal framework in France consisting of only one specific text and a single court decision, is at the moment largely untested[184].

On 24 May 2019, the Action Plan for Business Growth and Transformation law[185] (PACTE) entered in force, establishing a legal framework for both ICO and cryptocurrency related businesses (i.e. secondary market). PACTE

---

183 This position is to be handled with care since there are yet no relevant case law, no uniform tax practice and no unanimous doctrine. See Virtual Currency Regulation - Switzerland.

184 By a decision of 26 April 26 2018, the Council of State has specified the methods of taxation of gains resulting from the sale of Bitcoins by individuals. Samuel Martinet, French Crypto Regulation à la carte: Context, News, Perspectives, Coin Telegraph, 4.5.2018.

185 Act No. 2019-486 of 22.5.2019, JO 23.5.2019.

explicitly separates ICOs from securities offerings and applies only to utility tokens, i.e. tokens that do not fall under another existing regulation such as the securities prospectus regulation (in other words, securities offerings cannot be carried out under the form of an ICO). The interesting feature of PACTE is its non-mandatory approach: it introduces an optional approval for ICOs and an optional license for crypto-assets intermediaries while it strengthens AMF's powers as the regulator of the crypto industry. Thus, ICO issuers will not need to obtain approval from AMF before offering their tokens, and intermediaries will not have to be licensed to offer crypto services. The underlying idea is to encourage these providers to apply for approvals, by giving approved ICOs and licensed intermediaries certain legal rights. AMF's approval will be not issued to a person (token issuer) but to a transaction (ICO)[186].

ICO issuers may apply for approval if they are French resident, if necessary, through a subsidiary or a branch, provide adequate technical and financial information ('white paper'), set up an appropriate system to monitor and safeguard the assets collected, and implement due AML/KYC measures[187]. This resembles to a voluntary 'visa' system that incorporates the "best practices" advocated for by the French crypto-industry. The visa system can *de jure* split the ICO market between AMF approved ICOs and unregulated ICOs, which effect cannot be understated[188]. Uncertainties as regards legal framework for ICOs have led traditional FIs to be very wary of engaging in anything crypto-related businesses. Today, simple things such as opening a bank account can prove difficult for crypto-projects. The visa could enable legitimate ICOs to more easily interact with critical third parties such as banks, and also serves as a quality label which enables these companies to mass market their tokens and products to consumers in France and abroad. It is worth noting how innovative this voluntary approach appears internationally[189].

PACTE also strengthens the AMF's regulatory powers for an increased oversight of approved ICOs and licensed crypto service providers, that includes the publication of a blacklist of non-compliance organisations, and the closing down of fraudulent websites offering crypto services. Currently, the only AML requirement applies to crypto service providers offering to convert fiat money into cryptocurrencies or vice versa, thereby serving as an intermediary. Setting

186 Wolters Kluwer France, Actualités du droit, Interview of Anne Maréchal, 22.5.2019.

187 See art. 85, Act N° 2019-486.

188 See French Crypto Regulation à la carte.

189 Perchet/Loget/Daniel, Blockchain & Cryptocurrency Regulation 2019 ¦ France, Global Legal Insights.

up a full array of AML/CFT measures is necessary to obtain approval as a payment service provider. A new category of regulated service providers is created by PACTE: crypto service providers. Custodial services and brokers/dealers offering the "purchase or sale of digital assets against legal tender or other digital assets", and crypto exchange operators can opt to be licensed and placed under the supervision of the AMF[190]. Cryptoassets encompass both tokens[191] and traditional crypto-assets or cryptocurrencies. However, pursuant to 5th AMLD and FATF last recommendations AMF made it clear that a registration shall be mandatory for both custodians of cryptoassets and service providers for purchase or sale of virtual assets against legal tender. The requirements to obtain such registration will not be overly burdensome[192] whereas the optional licensing procedure impose more stringent requirements, similar to the licensing procedure of regulated investment services providers, in particular as regards AML procedures. The visa or license granted by the AMF has no extraterritorial effect and there is no 'passporting' regime with respect to ICOs and crypto-assets intermediaries. It is however expected that these provisions be modified once the FATF recommendations are updated, as the FATF will likely require that all crypto-related companies be subject to the AML legislation[193]. In addition, Article 41 of the Finance Bill 2019 introduced a reporting obligation to crypto accountholders opened in foreign institutions, for example virtual asset trading platforms or assimilated organisms[194]. This system applies to to tax returns filed on or after 1 January 2020 for natural persons, associations and companies that do not have the commercial form. French Minister of Economy and Finance announced during the Paris Blockchain Conference that France would support the adoption by the EU of a legislative framework similar to the one created by PACTE[195].

---

190 The scope of certain of these services, notably the custody and the purchase or sale of virtual assets services, is still unclear and should be clarified by an upcoming decree. De Vauplane/Charpiat, With the Enactment of the Loi PACTE, the French Regulatory Framework for Crypto-Activities and ICOs Becomes Effective, 29.5.2019.

191 As defined by the ICO regulation.

192 Managers and majority shareholders will be checked for "honorability" and sufficient experience, and the entity for the adoption of adequate AML procedures. See With the Enactment of the Loi PACTE.

193 See With the Enactment of the Loi PACTE.

194 France Loi N° 2018-1317 of 28 December 2018 de finances pour 2019 (1). FiscalOnline.com, Plus-value résultant de la cession de « bitcoins » réalisées par les particuliers : les obligations déclaratives sont précisées, published 14.1.2019.

195 Kevin Helms, France Adopts New Crypto Regulation, Bitcoin.com, 16.4.2019.

4.3 United States

The USA are not a contracting OECD AEoI state. Actually, CRS draws extensively on FATCA[196] that has been binding unilaterally since its enactment in 2010. CRS deviates from FATCA standard mainly driven by the multilateral nature of CRS system and FATCA's broader scope that holds a nexus based on citizenship[197] and a comprehensive withholding tax. FATCA defines two reporting information flows: certain U.S. taxpayers holding financial assets[198] outside the USA must report those assets to the Internal Revenue Service (IRS) and certain Foreign FIs (FFIs) must report directly or indirectly to the IRS data about financial accounts held by U.S. taxpayers or by foreign entities in which U.S. taxpayers hold a substantial ownership interest. In order to avoid legal obstacles in partnering countries, the USA signed with other governments two models of IGAs: Model 1 generally requires FFIs to report information to their respective government, which then automatically exchanges the information, on a reciprocal or nonreciprocal basis, with the USA pursuant to an income tax treaty or exchange of information agreement; Alternative Model 2, agreed by Switzerland and Japan, generally requires direct reporting by FFIs, after registration, to IRS[199].

The US is very strict in its approach to cryptoassets for compliance purposes. However, positions vary among federal agencies and between the 50 states, and this configuration has led to concurrent and overlapping regulatory jurisdictions and increasing scrutiny of intermediaries and trading platforms[200]:

– Financial Crimes Enforcement Network (FinCEN) considers crypto exchange 'money service businesses' (MSB), which means they are subject to existing banking regulations (AML/KYC, reporting requirements, etc);

– SEC regards certain cryptoassets issued as part of ICOs as securities[201], which generates a registration duty;

---

196 Model 1 Intergovernmental Agreements (IGA). See Standard for AEoI, Introduction #5.

197 US Departement of the Treasury, Resource Center, Foreign Account Tax Compliance Act.

198 With an aggregate value of more than the reporting threshold (at least $50'000). The Banks.eu, FATCA and European countries, 8.9.2015.

199 Supplemented with aggregate disclosure of "recalcitrant" accountholder data pursuant to exchange of information requests by IRS.

200 See An In-depth look at Bitcoin laws.

201 Under the Securities Act of 1933 and the Securities Exchange Act of 1934. See Standard for AEoI, Introduction #5.

– Commission Futures Trading Commission (CFTC) has designated certain cryptoassets as commodities that must be cleared in the same manner as other products. Clearing agencies must execute transfer ownership by book entry;

– IRS treats virtual currency as property[202] for income tax purposes. Consequently, a capital gain or loss upon disposition must be reported.

At the federal level, the Bank Secrecy Act (BSA) is the primary law that imposes AML obligations on certain enumerated FIs that are not otherwise federally regulated. It requires a registration duty with FinCEN, establishes risk-based AML programmes, and imposes data collection, maintenance and sharing with the federal body. On 9 May 2019, FinCEN issued rules intended to MSB, i.e. organisations that provide crypto custody services, perform exchange services, or issue cryptoassets; these entities are subject to 'money transmitter[203]' obligations under BSA. AML obligations are similar to those in EU posed upon crypto exchanges[204] that trade virtual-to-fiat currencies, and wallet providers that hold cryptoaccounts on behalf of their customers, effectively serving as banks offering current accounts on which fiat money can be deposited, stored, and transferred. As early as 2011, FinCEN laid a rule that covers money transmission of "other value that substitutes for currency", opening the doors for the assessment of 'money transmitters' services in cryptocurrencies. It published in 2013 an interpretative guidance[205] for crypto exchanges and set the principles for AML/KYC procedures. The guidance addresses convertible virtual currencies[206], which are 'transmitted' when transfers of value between persons or from one location to another occur, including the acceptance of real money from a user's bank account to fund a convertible virtual currency[207]. FinCEN applies the money transmitter laws in an extensive way to bring crypto exchanges into their supervisory remit. It has thus been involved in the first action taken against a non-US based exchange,

202 I.R.S. Notice 2014-21, 2014-16 I.R.B. 938. See p369, Virtual Currency Regulation - USA.

203 A money transmitter is any person or entity that provides money transmission services or is engaged in the transfer of funds. See p351, Virtual Currency Regulation - USA.

204 Sweeney/Karter, Insight: Specifically Identifying Exchange-Based Crypto: An Old Solution to a New Problem, Tax Bloomberg, 16.4.2019.

205 FIN-2013-G001, FinCEN Issues Guidance on Virtual Currencies and Regulatory Responsibilities, 18.3.2013. See 352, Sackheim/Howell, The Virtual Currency Regulation Review - Edition 1, United States, Law Reviews, November 2018.

206 Virtual currency that 'has either an equivalent value in real currency, or acts as a substitute for real currency". See p352, Virtual Currency Regulation - USA.

207 See p353, Virtual Currency Regulation - USA.

the Russian-domiciled BTC e-exchange, for a breach of US AML laws[208]. While FinCEN indicates that it does not expect an US cryptoholder on a foreign third-party exchange to disclose ownership, it is unclear whether those individuals would nonetheless need to report ownership to IRS[209]. In 2018, IRS designated cryptocurrency as its main focus and aims to address noncompliance through various treatment streams including taxpayer outreach and examinations by IRS. In 26 July 2019, the tax authority announced that it anticipates to reinforce measures in the near future. A forthcoming guidance is expected to address foreign asset ownership reporting[210].

At the state level, various approaches have been undertaken, particularly the regulation of exchanges or other money transmitters: specific licensing regimes applicable to cryptocurrency exchanges (e.g. New York BitLicense), or an inclusive approach with existing financial laws for crypto businesses. States regulations generally do not cover end users of cryptocurrency (e.g. for payments of goods and services or investors for their own portfolios) but target purchases and sales of cryptocurrencies 'on behalf of others[211]'. While usually not as extensive as specific regimes, inclusive legislation leaves room for additional controls by the states as a condition of entity licensing. A promising project is the Uniform Act that may become the basis for future legislation after its introduction in the legislatures of several states[212]. The Uniform Act includes licensing requirement, prudential regulations and customer protection rules relating to businesses engaged in activities involving exchanging, transferring or storing virtual currencies[213]. Rationale of Uniform Act is to provide a unified regulatory regime tailored to the specific issues relating to virtual currency businesses and foster legal certainty. A sister regulation, the Uniform Commercial Code[214], requires that cryptocurrencies credited to a

---

208 See p353, Virtual Currency Regulation - USA.

209 A reportable disposition occurs when exchanging a crypto-for-fiat currency or exchanging one cryptocurrency for another, or when using a cryptocurrency to pay for goods or services. IRS Notice 2014-21. P.1, IRS begins notifying owners of cryptocurrency of potential failures to report income and pay taxes, BakerMcKenzie Client Alert, 13.8.2019.

210 See p2, Murrer/O'Brien/Murray, IRS begins notifying owners of cryptocurrency.

211 See p347, Virtual Currency Regulation - USA.

212 Uniform Regulation of Virtual Currency Business Act has yet to be adopted. See p345, Virtual Currency Regulation - USA.

213 See p350, Virtual Currency Regulation - USA.

214 Unif. Reg. of Virtual-Currency Bus. Act (Unif. Law Comm'n 2017) (Uniform Law). See p373, Virtual Currency Regulation - USA.

securities account (as a financial asset) and regulated under the Uniform Act be held at a securities intermediary.

As regards regulatory aspects of ICOs, SEC issued a report[215] in July 2017 detailing its approach on whether an ICO constitutes a securities offering. SEC has hence a basis upon which to assert jurisdictions including extra-territorial outreach. SEC is also looking to crack down on all operations that do not employ a central headquarters or governing body. Using Blockchain to create a crypto exchange without having a central operations center, but on a "blockchain basis" only as "decentralised exchanges", does not remove the owner from serving in a responsible manner towards customers[216]. SEC requires securities trading venues, which most ICO are, to be performed on a registered alternative trading system or a national securities exchange. This obligation often comprises broker/dealer and any service provider that facilitate transactions in virtual currencies as securities. The court case *IRS v. Coinbase* constitutes a prominent example of US government actions. In February 2018, the Bitcoin exchange was ordered to provide taxpayer IDs, identification numbers, names and transaction records covering 2013 through 2015 for around 13'000 customers to IRS. The information received from Coinbase will likely form the basis of forthcoming criminal tax cases[217]. SEC also plans to hire contractors to run cryptocurrency full nodes, that is to seek the full ledgers since inception (the genesis block) and all derivative currencies (tokens) for several and most common blockchains. Previously, a covert piece of technology was developed by the US gouvernement that can extract raw internet data from fiber-optic cables information from Bitcoin users such as password, internet browsing activity, users' internet addresses, timestamps, and network ports[218]. This technology can be used to presumably gather much more than the information necessary to identify someone and link them to specific Bitcoin addresses and transactions, and it can do so without having to rely on crypto-exchanges. It is assumed that the *IRS v. Coinbase* case in 2016 has been

---

215 Section 21(a) Report. Baker McKenzie, Regulatory Aspects of Initial Coin Offerings (ICOs) in Switzerland, 2018.

216 According to Chief of the SEC's new cyber unit statement on 11 November 2018 "where humans are connected to a code, aka a smart contract". Nick Marinoff, SEC's Robert Cohen: exchange owners are responsible even if they're not around, Blockonomi, 13.11.2018.

217 As announced by Don Fort, IRS's Criminal Investigation Division Chief. See p2, IRS begins notifying owners.

218 Known as OAKSTAR, developed by National Security Agency (NSA) in 2013 but acknowledged in 2018 following leaks. Simon Chandler, Government Tracking of Crypto Is Growing, But There Are Ways to Avoid It, Coin Telegraph, 7.10.2018.

filed with the identities of an unspecified number of individuals associated with a number of cryptowallets. This summons was significant because it indicated that IRS could track certain wallets precisely enough to determine that they had been involved in the violation of US tax legislation, and that the wallets were attached to Coinbase[219]. It runs, therefore, another system that is less about cryptographic tool penetrating blockchains and more about simply assembling all the disparate threads of data strewn across the Internet.

V. Considerations for the future

Since the first rule among the cryptocurrency traders is not to use a financial intermediary, it is expected that most of the traffic will happen outside of the exchanges. Regulators cannot rely on financial intermediaries to enforce disclosure of cryptocurrencies, and if they cannot rely on financial intermediaries, disclosure regimes such as CRS cannot work. They must look elsewhere, and change their perspectives, while developing regulations and framework for disclosure of assets: the main challenge is being to keep up with the pace of innovation. On 31 August 2019, a prominent US investor warned "There is a growing realisation that the supply of fiat money is growing at a rapid pace not only because of central bank activities to drive down interest rates by printing more money but also because of the rapid and inexorable rise of cryptocurrencies. No one really knows how much cryptocurrency has been created. There is a whole generation of people who have faith in the internet and cryptocurrencies. They are beginning to realise that fiat currencies such as the U.S. dollar and euro really do not have anything behind them except the faith of the public. Given the increasing credibility and faith in cryptocurrencies, they will gain in favour as a currency, but there will always be a lingering doubt and the need for gold as a safe haven"[220]. The consequences of the financial crisis have not only resulted in the loss of confidence in the institutions, but also in the sometimes dubious and counterproductive inflation of regulations, as well as a drastic and global lowering of interest rates, which puts at risk an

---

219 Chainalysis, a Switzerland-based 'blockchain intelligence' provider cooperated with IRS in various cases thanks to its capability to use "data scraped from public forums, leaked data sources including dark web, exchange deposits and withdrawals to tag and identify transactions" and combine data made publicly available on blockchains with personal info carelessly left by cryptousers on the web. See Government Tracking of Crypto.

220 Reuters Global Markets Forum, Falling rates lead to irrational investments, eventual crash - Mark Mobius, 31.8.2019.

entire economic and financial model. Alternative models, whether cryptocurrencies or another, will find their way into these uncertainties as long as governments do not implement real measures to accompany them. First step can be raising awaress and education to prevent any 'misunderstanding' from cryptousers of the tax and regulatory aspects. Future developments such as regulated service providers offering digital identities (beyond the mere registration of information) can facilitate the investor screening process and verification. Introducing a customer digital ID would permit AML/KYC information in line with CRS to be shared with regulators (with consideration to privacy issues and related hacking and abuse risks as well as a balance between quality targets and quantity measures for AML purposes). Potential solutions would include the use of platforms on which only investors who satisfy investment criteria (e.g. accredited investors) are allowed to participate and the tokens used to gain access to the platform would contain an investor's certified digital identity[221]. Conversely, accredited intermediary similar to a banking licence or securities dealers' licences for crypto service providers[222] can ensure that the businesses are conducted in an orderly manner. Decentralised plateforms regulation could be principle-based, a combination of a control mechanism with a minimum set of principles[223]. Governments could provide supporting mechanisms whereby the consensus of users would enforce their own 'community standards'. The downside of this approach is that it may result in regulators allowing illegal or fraudulent activity to go unchecked. Accreditation practices may reveal critical since more banks are refusing to work with cryptocurrency trading platforms, including 'blockchain consultancies' or any firm using the terms 'crypto' or 'blockchain' in business filings[224]. By doing so, banks are precluding the sector but expose themselves to losing shares in the ever-growing crypto market. By forcing crypto-related service providers to quickly adapt and accelerate their integration into the 'real' economy, there is a risk of a parallel financial system based on blockchain technology that can function without banks and other FIs and challenge the existing regulatory systems.

---

221 Daniella Skotnicki, Blockchain: a path to innovation, Cayman Funds Magazine, 4.5.2018.

222 FINMA guidance: stringent approach to combating money laundering on the blockchain, Press release, 26.8.2019.

223 Ex. no back doors/loopholes or hidden functionalities, no white listing of malware, no fraudulent collusion, responsible cryptographic key management, and the pursuit of the state of the art. See p. 29, ECB Crypto-Assets Task Force and An In-depth look at Bitcoin.

224 Cali Haan, Dutch Banks Not Serving Blockchain Firms Due to Concerns About Money Laundering, 24.8.2019.

Yet, at the time of writing, the legal status of cryptoassets varied among countries, absent a common taxonomy of cryptoassets, and a shared understanding of how cryptoassets should be treated from a regulatory standpoint[225]. Given the global dimension of the cryptoassets phenomenon, fragmented and/or inconsistent regulatory approaches undertaken at the country level may prove ineffective and create incentives for regulatory arbitrage. The cryptocurrency industry is mainly opposed to large-scale regulation that would negatively affect the decentralised nature of the system and undermine the philosophy of the technology. In its view, creating a new regulatory and tax structure only for blockchain-based assets could result in significant expenses, which would be passed on to the taxpayer cryptouser, citing the example of regulatory inflation affecting the traditional financial sector since 2008. In the opinion of the author, some regulation is needed to legitimise and protect the technology and the market. Taking action such as applying the KYC/AML standards would achieve a twofold objective: protecting the state and the individual, as well as empowering companies active in Blockchain with their duties to their clients and investors. A framework of rules in respect of the blockchain industry would allow for companies and customers operating in the ecosystem to act on a level playing field. Also, it would help to raise industry standards, facilitate market access and prevent manipulation. The cryptocurrency sector is an exciting and growing field with great potential, in which many casual/amateur investors are in direct contact with experienced traders. Without regulation, some operators may be tempted to use their experience to manipulate the market. Without some certainty about regulation, it is unlikely that the required scalability of the technology will be able to occur. In every case, legal and tax certainty is for the benefits of all and would help states to achieve the ultimate goal of CRS: the taxation of offshore held assets.

225 See “Regulatory issues”, ECB Crypto-Assets Task Force.

VI. Bibliography

OECD (2017), Standard for Automatic Exchange of Financial Account Information in Tax Matters, Second Edition, OECD Publishing, Paris

OECD (2018), Standard for Automatic Exchange of Financial Information in Tax Matters - Implementation Handbook - 2nd Edition, OECD, Paris

OECD (2018), Model Mandatory Disclosure Rules for CRS Avoidance Arrangements and Opaque Offshore Structures, OECD, Paris

OECD (2019), International Exchange Framework for Mandatory Disclosure Rules on CRS Avoidance Arrangements and Opaque Offshore Structures, OECD, Paris.

EUROPEAN CENTRAL BANK (ECB) Crypto-Assets Task Force, Occasional Paper Series, Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures, No 223/May 2019

EUROPEAN SECURITIES AND MARKETS AUTHORITY (ESMA) Advice Initial Coin Offerings and Crypto-Assets, ESMA50-157-1391, 9.1.2019

FATF (2019), Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris

FATF (2012-2019), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France

GLOBAL FORUM ON TRANSPARENCY AND EXCHANGE OF INFORMATION FOR TAX PURPOSES, Automatic Exchange of Financial Account Information, Background Information Brief, Update January 2016

EUROPEAN COMMISSION, Communication from the Commission to the European Parliament and the Council, Towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework, COM(2019) 360 final, 24.7.2019

COUNCIL OF EUROPEAN UNION, Council Directive 2018/822/EU (DAC6) of 25 May 2018, amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation in relation to reportable cross-border arrangements

SWISS FEDERAL COUNCIL, Legal framework for blockchain and distributed ledger technology in the financial sector, Bern, 14.12.2018

SWISS FEDERAL DEPARTEMENT OF FINANCE, SIF's position of 16 April 2018 on the introduction of disclosure rules for intermediaries along the lines of the OECD model rules.

SWISS FINANCIAL MARKET SUPERVISORY AUTHORITY, Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs), 16.2.2018

SWISS FINANCIAL MARKET SUPERVISORY AUTHORITY, FINMA guidance: stringent approach to combating money laundering on the blockchain, Press release, 26.8.2019

SWISS FINANCIAL MARKET SUPERVISORY AUTHORITY, FINMA Guidance 02/2019, Payments on the blockchain, 26.8.2019

SWISS STATE SECRETARIAT FOR INTERNATIONAL FINANCE, Federal Council wants to further improve framework conditions for blockchain, 14.12.2018

SWISS STATE SECRETARIAT FOR INTERNATIONAL FINANCE, Federal Council initiates consultation on improving framework conditions for blockchain/DLT, 22.3.2019

SWISS STATE SECRETARIAT FOR INTERNATIONAL FINANCE / SWISS FINANCIAL MARKET SUPERVISORY AUTHORITY, Consultation on the work of the Working Group Blockchain / ICO, 2018

SWISS REPORT OF THE INTERDEPARTEMENTAL COORDINATING GROUP ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM (CGMF), National Risk Assessment (NRA): Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding, October 2018

SWISS FEDERAL ACT ON COMBATING MONEY LAUNDERING AND TERRORIST FINANCING (AMLA) of 10 October 1997 (Status as of 1 January 2019)

IBFD, Digital Economy, Dispute Resolution & Blockchain Technology dominate 12th edition of IFA Mauritius conference, 24.5.2018

WOLTERS KLUWER FRANCE, Actualités du droit, Interview of Anne Maréchal, 22.5.2019

JONATHAN SCHWARZ, Tax certainty: Cure the disease not the symptom, Kluwer International Tax Blog, 28.8.2018

ANDRES KNOBEL, commissioned by the Greens/EFA Group in the European Parliament, Reporting taxation: Analysing loopholes in the EU's automatic exchange of information and how to close them, 15.10.2018

JOSH WHITE, Banks feel the strain of getting ready for DAC6, International Tax Review, 25.1.2019

BACHARACH JEREMY, Cryptoactifs : La Communication 02/19 a-t-elle une base légale suffisante ? Centre de droit bancaire et financier, 2.9.2019 https://www.cdbf.ch/1082/

PERCHET/LOGET/DANIEL, Blockchain & Cryptocurrency Regulation 2019 | France, Global Legal Insights

CARLOS SANTISO, Can blockchain help in the fight against corruption? World Economic Forum, 12.3.2018 (weforum.org/agenda/2018/03/will-blockchain-curb-corruption, last visit 23.3.2019)

THOMAS WAHL, 5th Anti-Money Laundering Directive, Eucrim, 20.10.2018 (eucrim.eu/news/5th-anti-money-laundering-directive, last visit 30.7.2019)

FAVRE/HOUDROUGE/ELSENER, The Virtual Currency Regulation Review - Edition 1, Switzerland, Law Reviews, November 2018

SACKHEIM MICHAEL/HOWELL NATHAN, The Virtual Currency Regulation Review - Edition 1, The United States, Law Reviews, November 2018

MURRER/O'BRIEN/MURRAY, IRS begins notifying owners of cryptocurrency of potential failures to report income and pay taxes, BakerMcKenzie Client Alert, August 2019

REUTERS GLOBAL MARKETS FORUM, Falling rates lead to irrational investments, eventual crash - Mark Mobius, 31.8.2019 (in.reuters.com/article/gmf-emergingmarkets-mobius/qa-falling-rates-lead-to-irrational-investments-eventual-crash-mark-mobius-idINKCN1VL0G3, last visit 15.9.2019)

ANDREW NORRY, An In-depth Look at Bitcoin Laws & Future Regulation, Blockonomi, 2.7.2018 (blockonomi.com/bitcoin-regulation, last visit 10.6.2019)

NICK MARINOFF, SEC's Robert Cohen: exchange owners are responsible even if they're not around, Blockonomi, 13.11.2018 (blockonomi.com/decentralized-exchange-owners-responsible, last visit 5.9.2019)

NICOLA FILZMOSER, Governments track the crypto space, Blockpit, 13.3.2019 (blog.blockpit.io/en/authority-crypto-regulations, last visit 5.9.2019)

KEVIN HELMS, France Adopts New Crypto Regulation, Bitcoin.com, 16.4.2019 (news.bitcoin.com/france-cryptocurrency-regulation, last visit 3.8.2019)

YOGITA KHATRI, US SEC seeking big data tool for major blockchains, CoinDesk, 4.2.2019 (coindesk.com/sec-seeks-big-data-tool-for-blockchains-to-improve-compliance, last visit 5.9.2019)

MAX GANADO, Blockchain: Some legal considerations relating to Security Token Issuance, 12.7.2019

SIMON CHANDLER, Government Tracking of Crypto Is Growing, But There Are Ways to Avoid It, Coin Telegraph, 7.10.2018 (cointelegraph.com/news/government-tracking-of-crypto-is-growing-but-there-are-ways-to-avoid-it, last visit 5.9.2019)

LUKAS HOFER, FATF Publishes New Crypto Guidelines - Threat or Opportunity? 24.6.2019 (ico.li/fatf-publishes-new-crypto-guidelines, last visit 23.8.2019).

MARCO CAVICCHIOLI, FATF recommendations for crypto could favour DEXs, The Cryptonomist, 24.6.2019 (en.cryptonomist.ch/2019/06/24/fatf-recommendations-for-crypto, last visit 21.8.2019)

FINTECHNEWS, Tokenized Equity: A Revolution For Traditional And New Capital Markets, 14.12.2018 (fintechnews.ch/blockchain_bitcoin/tokenized-equity-a-revolution-for-traditional-and-new-capital-markets/24371/, last visit 31.7.2019)

And I would like to express my warm thanks to blockchain and compliance experts who shared their knowledge and experience:

AZANGAR SOLOMON, Cryptocurrency Advisor; BAUR JEANNE, International Banking Operation Specialist; BALTENSPERGER JÜRG, Blockchain Compliance.

VII. Table of abbreviations

AEOI	Automatic Exchange of Information in Tax Matters
AMF	French Financial Market Authority (Autorité des marchés financiers)
AMLA / AMLD	Swiss Anti-Money Laundering Act / European Anti-Money Laundering Directive
BO	Beneficial Ownership or Beneficial Owner
CEU / EU	Council of the European Union / European Union
CTF	Counter-Terrorism Financing/Fundraising
CRS	Common Reporting Standard
EP	European Parliament
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
FFI / FI	Foreign / Financial Institution
FINMA	Swiss Financial Market Supervisory Authority
FTA	Swiss Federal Tax Administration
ICO	Initial Coin Offering
INR	Interpretive Note to Recommendation
IRS	US Internal Revenue Service
KYC	Know your customer
MBS	Money Service Business
MCAA	Multilateral Competent Authority Agreement on the Automatic Exchange of Financial Account Information
MCAATM	Multilateral Convention of Administrative Assistance in Tax Matters
OECD	Organisation for Economic Co-operation and Development
SEC	US Securities and Exchange Commission