

UNDERSTANDING DIGITAL TOKENS

Legal Landscapes Governing Digital Tokens in the European Union



Prepared by the Token Alliance – an industry initiative of the Chamber of Digital Commerce

MAY 2021

Chamber Of Digital Commerce







The Chamber of Digital Commerce is the world’s largest trade association representing the blockchain industry. Our mission is to promote the acceptance and use of digital assets and blockchain technology.

Through education, advocacy, and working closely with policymakers, regulatory agencies, and industry, our goal is to develop a pro-growth legal environment that fosters innovation, jobs, and investment.

Token Alliance

The Token Alliance is an industry-led initiative of the Chamber of Digital Commerce, developed to be a key resource for the emerging industry surrounding the generation and distribution of tokens using blockchain technology. Comprised of more than 400 industry participants, the Alliance includes blockchain and token and legal experts, technologists, economists, former regulators, and practitioners from around the globe.

CHAMBER OF DIGITAL COMMERCE INDUSTRY INITIATIVES AND WORKING GROUPS

 <p>Smart Contracts Alliance Promotes real-world application of smart contracts to enhance the way business is conducted.</p>	 <p>Global Blockchain Forum Working with the world’s leading blockchain policy experts to develop industry best practices and help shape global regulatory interoperability.</p>
 <p>Blockchain Intellectual Property Council Balancing the protection of proprietary information with the openness necessary for innovation.</p>	 <p>Blockchain Alliance The public-private forum for the blockchain community and law enforcement to help combat criminal activity.</p>
 <p>Digital Assets Accounting Consortium Developing accounting and reporting standards for digital assets and blockchain technology.</p>	 <p>State Working Group Engaging with state and local governments on the regulation and implementation of blockchain technology.</p>

Acknowledgments

Blanca Escribano	Partner, EY Law Spain
Darko Stefanoski	Partner, EY Law Switzerland
Dennis Post	Partner, EY Tax Netherlands
José María Chozas	Senior, EY Law Spain
Kristina Miggiani	Fintech Lawyer & AML/CFT Specialist
Linn Anker-Sørensen	Senior Manager, EY Law Norway
Magnus Jones	Senior Manager, EY Tax Norway
Orkan Sahin	Manager, EY Law Switzerland
Tomasz Nowotny	Manager, EY LMS Poland

Contents

I.	Introduction – The Regulatory Framework For Digital Tokens In The EU	7
II.	A Legal Taxonomy For Digital Tokens In The EU	9
III.	Digital Tokens Within The EU Financial Regime	11
	A. DIGITAL TOKENS QUALIFYING AS “E-MONEY”	11
	1. Legal qualification under EMD2	11
	2. Practical considerations for tokens qualifying as e-money	12
	B. DIGITAL TOKENS AS “FINANCIAL INSTRUMENTS”	12
	1. Legal qualification under MiFID2	13
	1.1 National approach to legal qualification of Securities tokens	14
	1.2 ESMA's approach to legal qualification	14
	2. Legal framework potentially applicable to Securities tokens	15
	3. Practical considerations for service providers	18
	3.1 Offering of Securities tokens	18
	3.2 Secondary market trading: admission to trading	22
	3.3 Secondary market trading: trading platforms	23
	3.3.1 General approach	23
	3.3.2 Practical considerations for trading venues	24
	C. DLT TRANSFERABLE SECURITIES	26
	D. EC PROPOSAL ON REGULATED TOKENS	26
	1. Guidance on how existing legislation applies to crypto assets	27
	2. Potential targeted amendments to existing financial services legislation	27
	3. Pilot Regime	27
IV.	Digital Tokens Outside The EU Financial Regime	28
	A. INTRODUCTION: PROPOSAL FOR A REGULATION ON MARKETS IN CRYPTO-ASSETS REGULATION	28
	B. CLASSIFICATION OF DIGITAL TOKENS IN THE MICA REGULATION PROPOSAL	29
	1. Utility tokens	29
	2. E-money tokens	30
	3. Asset-referenced tokens	30
	C. REQUIREMENTS ON ISSUERS OF CRYPTO-ASSETS, ASSET-REFERENCED TOKENS, AND E-MONEY TOKENS	31
	D. SERVICE PROVIDERS SUBJECT TO AUTHORIZATION	31
	E. SPECIFIC CONSIDERATIONS REGARDING STABLECOINS	32
	1. Legal qualification of stablecoins	32
	2. Practical considerations	33
V.	Other Relevant Legal Considerations For Digital Tokens: Tax Considerations	34
	A. BLOCKCHAIN, DIGITAL TOKENS, AND TAXATION OF TOKENS	34
	B. EU AND TAXATION: HOW TO USE BLOCKCHAIN TO CREATE MORE ROBUST TAX SYSTEMS	36
	1. General comments	36
	2. VAT and customs	37
	3. Other taxes	38
	C. TAX TREATMENT – IDENTIFYING GENERAL STARTING POINTS	38
	1. Classification of tokens as a precondition for taxation	38
	2. Taxable events	39
	3. Remaining challenges	41
	D. CASE STUDY – DECENTRALISED FINANCE	42
VI.	Digital Tokens Outside The EU Financial Regime: AML Considerations	43
	A. INTRODUCTION	43
	B. AMLD5 – OVERVIEW	44
	1. Definition of VC	45
	2. Who or what does AMLD5 regulate?	45
	3. VC Exchanges	46
	4. VC Custodian Wallet Providers	48
	5. Gaps left by AMLD5	49
	C. FATF	51
	D. ENFORCEMENT AND COORDINATION	53
	E. FUTURE TRENDS TO LOOK OUT FOR	56
	F. QUO VADIS?	57
VII.	Conclusion	58

I. Introduction – The Regulatory Framework For Digital Tokens In The EU

A uniform regulatory framework for digital tokens¹ is currently under construction in the European Union (“EU”). Beginning in 2018, the European Commission (“EC”) started a process of research and consultation to assess the need to regulate in this realm, culminating in an action plan to create a pan-European unified regulatory framework. This action plan sits on the following building blocks:

- » adoption of non-legislative measures which would provide guidance on how existing legislation applies to digital tokens;
- » a pilot regime for distributed ledger technology (“DLT”) market infrastructures for digital tokens that qualify as financial instruments; and
- » a bespoke regime for the issuance and operation with digital tokens falling outside the financial services regulatory framework.

On the way to this action plan, it is worth mentioning a few milestones to get some context:

- » In 2017, ESMA issued two statements on initial coin offerings (“ICOs”)² alerting investors of associated risks (a high risk of total investment loss, lack of investor protection laws and vulnerability to fraud and money laundering) and stressing that involved companies should consider carefully if their activities were subject to regulation (e.g., determining whether tokens issued during ICOs qualified as “financial instruments”).
- » The Fintech Action Plan in 2018³ paved the route for important works assessing the applicability and suitability of the EU’s financial services regulatory framework to crypto-assets⁴. As a result, in 2019, the European Securities Markets Authority (“ESMA”) delivered advice to EU financial institutions on ICOs and crypto-assets (“ESMA Report”)⁵ in which it highlighted a number of regulatory concerns (in particular, difficulty in interpreting the rules within the context of digital tokens, inadequacy of such rules for that context, lack of regulation for digital tokens not constituting “financial instruments” which meant, e.g., that investors were exposed to substantial risks), noting that a common EU approach is the best way to address these concerns.
- » On the same day ESMA delivered its advice, the European Banking Authority (“EBA”) published a report for the EC on crypto-assets⁶ (“EBA Report”). In its view, digital tokens typically remained outside the scope of

1 In the European Union, the legal term to refer to digital tokens is “crypto-asset”, whose use is now well entrenched in the EU’s legal acquis after the term was used in legislative proposals (See Article 3(1)(2) of the MiCA Regulation Proposal). Nevertheless, for the purposes of this report, we will use the term “digital token” or “token” to refer to these assets, with the meaning of “transferable units generated within a distributed network that tracks ownership of the units through the application of blockchain technology”.

2 See <https://www.esma.europa.eu/press-news/esma-news/esma-highlights-ico-risks-investors-and-firms>.

3 European Commission (EC). (2018), Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic And Social Committee and the Committee of the Regions. FinTech Action plan: For a more competitive and innovative European financial sector. Retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0109>.

4 Crypto-asset is defined in the MiCA Regulation Proposal, Article 3(1)(b), as “a digital representation of value or rights, which may be transferred and stored electronically, using distributed ledger or similar technology”.

5 European Securities and Markets Authority. (2019). Advice Initial Coin Offerings and Crypto-Assets. Retrieved from <https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection>.

6 European Banking Authority. (2019). Report with advice for the European Commission on crypto-assets. Retrieved from <https://eba>.

EU financial services regulation. At the same time, unharmonized regulatory approaches were emerging throughout the EU, creating risks related to consumer protection, operational resilience, market integrity, money laundering, and a level playing field.

- » In this context, the EC launched a public consultation (“EC Consultation”) on an *EU framework for markets in crypto-assets*, completed from 19 December 2019 to 19 March 2020⁷, stressing the need for “a common approach with member states on cryptocurrencies to ensure [they] understand how to make the most of the opportunities they create and address the new risks they may pose”⁸. The EC Consultation was followed by a webinar on 13 May 2020 that showed the EC’s intention to regulate, at least to some extent, the intersection between the crypto-asset and the financial space, despite frontal opposition from a number of stakeholders. Following extensive feedback from the industry and regulatory authorities from around the world, the EC issued a “Non-paper⁹ on the legislative proposals for an EU framework for markets in crypto-assets” in May 2020¹⁰, later updated in July 2020¹¹. outlining possible actions to develop an EU regulatory framework on crypto-assets.
- » As a result, in September 2020, the EC released two legislative proposals as a first step of its unified framework for crypto-assets: the proposal for a regulation on Markets in Crypto-assets (“MiCA Regulation Proposal”)¹² and the proposal for a regulation on a pilot regime for market infrastructures based on distributed ledger technology (“Pilot Regime Proposal”)¹³.

The aim of this report is to help industry players and legal professionals to navigate the complex regulatory framework for digital tokens in the EU. With this purpose, this report will take us through the following topics:

- » *A legal taxonomy for digital tokens in the EU*: this section will explore a legal taxonomy of tokens in the EU based on the categorization of digital tokens presented by the EC Consultation and the token categories laid down in the regulation proposals.
- » *Digital tokens inside the EU financial regime*: this section studies the legal requirements applicable to digital tokens that may qualify as “financial instruments” under the Markets in Financial Instruments Directive II (“MIFID2”)¹⁴ or as “e-money” under the Electronic Money Directive (“EMD2”)^{15, 16}.

europa.eu/eba-reports-on-crypto-assets.

7 European Commission. (2019), Consultation Document on an EU framework for markets in crypto-assets. Retrieved from https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-crypto-assets-consultation-document_en.pdf.

8 Mission letter of President-elect Von der Leyen to Vice-President Dombrovskis, 10 September 2019.

9 A non-Paper is a discussion document designed to stimulate debate on a particular issue without representing the official position of the institution which drafted it.

10 European Commission (EC). (2020), Non-paper on the legislative proposals for an EU framework for markets in crypto-assets. Retrieved from https://www.politico.eu/wp-content/uploads/2020/05/May-14_3.pdf.

11 European Commission (EC). (2020), Non-paper on the legislative proposals for an EU framework for markets in crypto-assets, July update. Retrieved from https://drive.google.com/file/d/1ZBI_YSUcKbJCrSotoQk66z4jtd7Dvkj/view.

12 Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1600947409472&uri=COM:2020:593:FIN>.

13 Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology, <https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1600960374694&uri=COM:2020:594:FIN>.

14 Markets in Financial Instruments Directive II (2014/65/EU).

15 Electronic Money Directive (2009/110/EC).

16 A “directive” is an EU legislative act that sets out a goal that all EU countries must achieve establishing a common minimum level playing field across EU member states. However, it is up to the individual countries to devise their own laws on how to reach these goals. In

- » *Digital tokens outside the EU financial regime*: this section presents briefly the main lines of a regulation designed by the EC to regulate digital tokens falling outside the perimeter of existing financial services regulations.
- » *Other relevant legal considerations for digital tokens: tax considerations*: this section explores relevant tax considerations applicable to digital tokens.
- » *Other relevant legal considerations for digital tokens: AML considerations*: this section navigates the legal requirements applicable to digital tokens with the purpose of combatting money laundering and terrorism financing, mainly subject to the 5th Anti-Money Laundering Directive (“AMLD5”)¹⁷.

II. A Legal Taxonomy For Digital Tokens In The EU

A legal classification of digital tokens does not currently exist at an EU level, but this may change if the MiCA Regulation Proposal is enacted. It is possible, nevertheless, to draw a provisional taxonomy based on the EC Consultation¹⁸ and the MiCA Regulation Proposal.

Digital tokens are firstly categorized as “regulated” and “unregulated”. Regulated digital tokens are defined by the fact that they fall within the scope of the existing EU financial services regime. There are three types of regulated digital tokens:

- » Digital tokens qualifying as e-money, subject to EMD2, as explained in Section III(A).
- » “Securities tokens”, subject to the financial services regulatory package, as explained in detail in Section III(B).¹⁹
- » “DLT transferable securities”, subject to the Pilot Regime Proposal, as explained in Section III(C).²⁰

Unregulated digital tokens are those falling outside the perimeter of the EU financial services regime. This category encompasses a wide variety of digital tokens, normally utility and payment-type crypto-assets, as well as crypto-assets with a hybrid function.

Note that the term unregulated does not mean that these digital tokens are outside the scope of any EU legislation but merely that the financial services regulation framework does not apply to them. For instance, payment tokens will normally fall under the definition of “virtual currency” and thus subject to AML/CFT provisions²¹. Likewise, the sale of unregulated digital tokens to a public qualifying as “consumers” will trigger the application of the EU package on consumer protection. Tax considerations

contrast, a “regulation” is a binding legislative act. It must be applied in its entirety across the EU.

17 5th Anti-Money Laundering Directive (Directive 2018/843/EU).

18 The EC Consultation embraced the well-known Swiss Financial Market Supervisory Authority’s (“FINMA”) categorization, where crypto-assets are divided into three main categories, based on their economic function: “payment tokens” that may serve as a means of exchange or payment for a product or a service, “investment/asset tokens” that may have profit-rights attached to it and “utility tokens” that may enable access to a specific product or service. A fourth category would be the “hybrid crypto-asset”, reserved for those crypto-assets serving more than one of the previous economic purposes at the time or that might have its features altered throughout their lifecycle.

19 “Securities tokens” are a type of digital tokens that qualify as a financial instrument under Article 4(1)(44) MiFID2.

20 “DLT transferable securities” is defined in Article 5 of the Pilot Regime Proposal as transferable securities within the meaning of Article 4(1)(44) (a) and (b) of Directive 2014/65/EU that are issued, recorded, transferred, and stored using a DLT.

21 5th Anti-Money Laundering Directive (Directive 2018/843/EU).

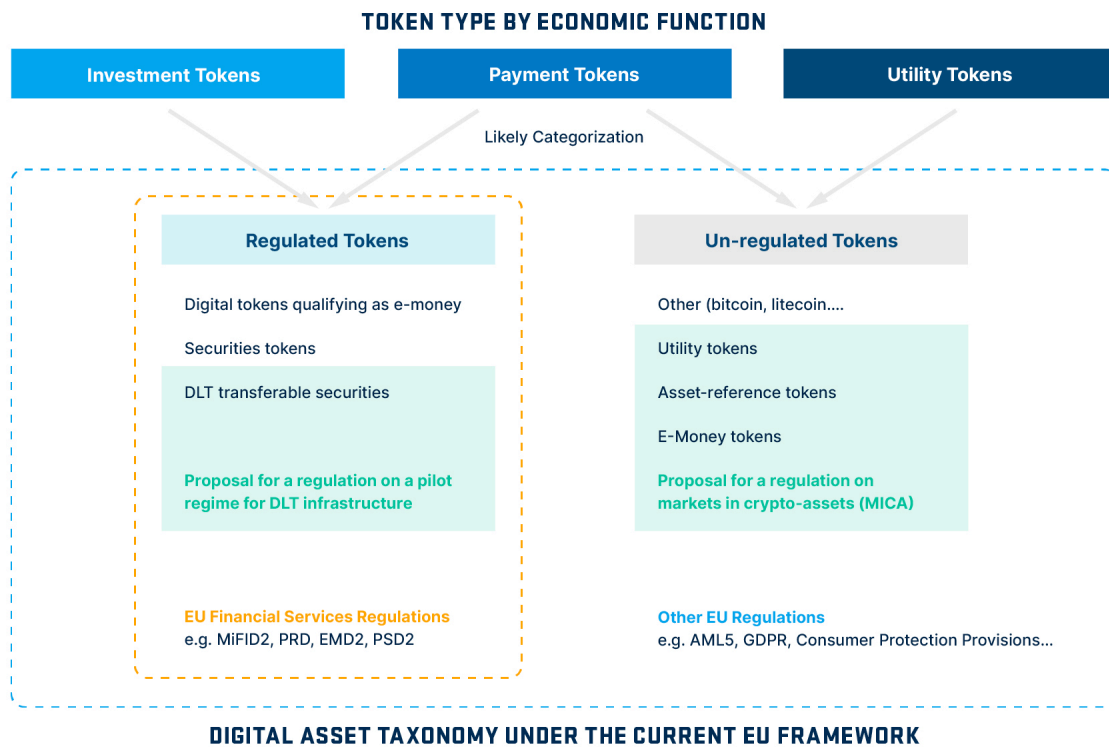
are also a relevant legal angle when analysing the legal implications attached to the operation with digital tokens.

Most notably, the EC released the MiCA Regulation Proposal to regulate certain aspects related to the issuance and operation with unregulated tokens. According to the proposal, there are three types of unregulated digital tokens:

- » “Utility token”.²²
- » “E-money token”.²³
- » “Asset-referenced token”.²⁴

Please consult Section IV for more information on the issuance and operation with unregulated tokens.

Chart 1. – Basic digital token categorization combining the EC Consultation, the MiCA Regulation Proposal, and the Pilot Regime Proposal.



Note: this chart showcases the EC Consultation’s conceptual framework to approach a classification of digital tokens, completed with the MiCA and the Pilot Regime Regulation Proposals. Note, nevertheless, that this is not set in EU law.

22 “Utility token” is defined in Article3(1)(5) of the MiCA Regulation Proposal as a type of crypto-asset which is intended to provide digital access to a good or service, available on DLT, and is only accepted by the issuer of that token.

23 “E-money token” is defined in Article3(1)(4) of the MiCA Regulation Proposal as a type of crypto-asset the main purpose of which is to be used as a means of exchange and that purports to maintain a stable value by referring to the value of a fiat currency that is legal tender.

24 “Asset-referenced token” is defined in Article 3(1)(3) of the MiCA Regulation Proposal as a type of crypto-asset that purports to maintain a stable value by referring to the value of several fiat currencies that are legal tender, one or several commodities or one or several crypto-assets, or a combination of such assets.

III. Digital Tokens Within The EU Financial Regime

A. DIGITAL TOKENS QUALIFYING AS “E-MONEY”

1. Legal qualification under EMD2

Electronic money or “e-money” is a digital alternative to cash. From an EU legal perspective, it can be broadly defined as an electronic store of monetary value on a technical device, such as a card, a phone, or software, that may be used for cashless payments to individuals or entities other than the e-money issuer. E-money products can be hardware-based or software-based, depending on the technology used to store the monetary value. Typical examples could be a prepaid payment card, an account-based scheme like PayPal, the value on a debit card, or even a bank deposit, in some cases²⁵.

EMD2 sets out the rules for the business practices and supervision of e-money institutions. A digital token will qualify as e-money to the extent that it satisfies each element of its legal definition in EMD2:

- » Electronically stored monetary value.
- » Represented by a claim on the issuer.
- » Issued on receipt of funds for the purpose of making payment transactions to individuals or entities other than the e-money issuer.

EU national financial authorities and industry groups have reported a handful of cases where payment tokens could qualify as e-money, e.g., tokens pegged to a given currency and redeemable at par value at any time²⁶. For instance, the European Association of Cooperative Banks (“EACB”) in its response to the EC Consultation (“EACB Response”)²⁷, identified Utility Settlement Coin as a deposit, falling under the concept of e-money.

The UK Financial Conduct Authority (“FCA”) stated in its *Guidance on Crypto-assets* (“FCA Report”), when it was a EU member state, that payment tokens such as bitcoin, ether, and others are unlikely to represent e-money because, amongst other things, they are not usually centrally-issued on the receipt of funds, nor do they represent a claim against an issuer²⁸. Furthermore, the FCA considers that digital tokens that establish a new sort of unit of account rather than representing fiat funds are unlikely to amount to e-money unless the value of the unit is pegged to a fiat currency²⁹.

25 FCA (2013). FCA Handbook: PERG 3A.3 The definition of electronic money. Retrieved from: <https://www.handbook.fca.org.uk/handbook/PERG/3A/3.html>.

26 EBA Report, p. 13-14.

27 European Association of Co-operative Banks. (2019). EACB response to the EC’s Online Public Consultation on an EU framework for markets in crypto-assets. Retrieved from: http://v3.globalcube.net/clients/eacb/content/medias/publications/position_papers/digitalisation_and_the_use_of_data/2020/final_eacb_ec_public_consultation_on_an_eu_framework_for_markets_in_crypto_assets.pdf, p. 4.

28 Financial Conduct Authority (FCA). (2019). *Guidance on Cryptoassets*, July version. Retrieved from: <https://www.fca.org.uk/publication/consultation/cp19-03.pdf>, p. 31.

29 *Ibid.*, p. 45.

A practical example of qualifying as an e-money token and meeting the criteria of EMD2 is identified in the EBA Report³⁰. The example includes a token created by a company in the context of transferring donations to a charity based on DLT. When in receipt of fiat donations in a segregated bank account, the company creates a token representing the received donations. This token is then deposited in the donor’s wallet, ready to be pledged to a specific charity or redeemed at par value. This means that no direct exchange of donations occurs between the donor and the charity in a closed environment.

It is important to highlight that digital tokens that qualify as e-money are different from “e-money tokens” as defined in the MiCA Regulation Proposal. We will explore this later, under Section IV(B).

2. Practical considerations for tokens qualifying as e-money

Where a digital token would qualify as e-money, authorisation as an e-money institution is required to carry out activities involving e-money tokens pursuant to the EMD2, unless an exemption applies.

Further, payment services leveraging e-money tokens could also be covered by the Payment Services Directive (PSD2)³¹. PSD2 applies to payment services enabling placing, transferring, or withdrawing funds, where the term “funds” means banknotes, coins, scriptural money, or e-money. Taking into account that digital tokens are not banknotes, coins, or scriptural money, digital tokens do not fall within the perimeter of the PSD2 unless they qualify as e-money for the purposes of the EMD2. Should a firm propose to carry out, using DLT, a “payment service” as defined in the PSD2 with an e-money token, such activity would fall within the scope of the PSD2 by virtue of being “funds”³².

Where organizations would like to also provide payment services, they must obtain the corresponding authorisation, which can be simultaneously managed with the e-money authorisation before the EBA³³.

B. DIGITAL TOKENS AS “FINANCIAL INSTRUMENTS”

This section analyses the qualification of some digital tokens as financial instruments under the current EU financial services law. To avoid a very extensive report, the analysis is focused on the potential application of MiFID2 and the Prospectus Regulation (“PR”)³⁴ to agents dealing with digital tokens. It is important to note that other EU financial legislation is potentially applicable to digital tokens. This section does not intend to cover those exhaustively but merely points to its applicability

³⁰ EBA Report, p.13.

³¹ Payment Services Directive 2 (2015/2366/EU). PSD2 puts in place comprehensive rules for payment services and payment transactions. In particular, the PSD2 sets out rules concerning: (i) strict security requirements for electronic payments and the protection of consumers’ financial data, promoting safe authentication, and reducing the risk of fraud; (ii) the transparency of conditions and information requirements for payment services; (iii) the rights and obligations of users and providers of payment services.

³² EBA Report, p.14.

³³ EBA (2017). Final report on the EBA Guidelines under Directive (EU) 2015/2366 (PSD2) on the information to be provided for the authorisation of payment institutions and e-money institutions and for the registration of account information service providers. Retrieved from: [https://eba.europa.eu/sites/default/documents/files/documents/10180/1904583/f0e94433-f59b-4c24-9cec-2d6a2277b62c/Final%20Guidelines%20on%20Authorisations%20of%20Payment%20Institutions%20\(EBA-GL-2017-09\).pdf](https://eba.europa.eu/sites/default/documents/files/documents/10180/1904583/f0e94433-f59b-4c24-9cec-2d6a2277b62c/Final%20Guidelines%20on%20Authorisations%20of%20Payment%20Institutions%20(EBA-GL-2017-09).pdf).

³⁴ Prospectus Regulation (2017/1129/EU).

as per EU consultation and other relevant bodies commenting upon this in relation to digital tokens. For further reference, Chart 2 below offers a general overview of all the financial regulations that are potentially applicable with a brief summary of the regulations' scope and a note on their applicability to digital tokens.

1. Legal qualification under MiFID2

MiFID2 is a cornerstone of the EU's regulation of financial markets seeking to improve their competitiveness by creating a single market for investment services and activities and to ensure a high degree of harmonised protection for investors in financial instruments.

To summarise, MiFID2 sets out:

- (i) conduct of business and organisational requirements for investment firms;
- (ii) authorisation requirements for regulated markets, multilateral trading facilities, organised trading facilities and broker/dealers;
- (iii) regulatory reporting to avoid market abuse;
- (iv) trade transparency obligations for equity and non-equity financial instruments; and
- (v) rules on the admission of financial instruments to trading. MiFID2 also contains the harmonised EU rulebook on investor protection, retail distribution and investment advice³⁵.

MiFID2 provides a list of instruments qualifying as financial instruments under its perimeter, including, *inter alia*, transferable securities, money market instruments, units in collective investment undertakings and various derivative instruments. Depending on their specific features, digital tokens could qualify as some of these instruments, especially as transferable securities. For the purposes of this report, tokens qualifying as transferable securities or other financial instrument are referred to as "Securities tokens".

The term "transferable securities" is defined as those "*classes of securities which are negotiable on the capital market, with the exception of instruments of payment, such as:*

- » *shares in companies and other securities equivalent to shares in companies, partnerships or other entities, and depositary receipts in respect of shares;*
- » *bonds or other forms of securitised debt, including depositary receipts in respect of such securities; and*
- » *any other securities giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities, currencies, interest rates or yields, commodities or other indices or measures*"³⁶.

³⁵ EC Consultation, p. 32.

³⁶ Article 4(1)(44) MiFID2.

1.1 National approach to legal qualification of Securities tokens

Despite the common framework established by MiFID2, the actual classification of a digital token as a financial instrument is the responsibility of the financial authorities in each member state and will depend on the specific national implementation of EU law based on the information and evidence provided to that EU national financial authority³⁷. As a result, member states might reach different conclusions when assessing the legal classification of a Securities token, posing new challenges to adopting a common regulatory and supervisory framework across the EU. Furthermore, the current situation challenges the capacity of financial authorities to interpret the regulatory framework consistently, which increases the risk of regulatory arbitrage.

1.2 ESMA's approach to legal qualification

In ESMA's survey of EU's national financial authorities, the majority of the respondents agreed that the existence of attached profit rights (whether or not alongside ownership or governance rights) was sufficient for a digital token to constitute a transferable security, provided the digital token was freely tradable and did not function as a payment instrument³⁸.

Notably, ESMA excluded pure payment tokens (such as bitcoin, ether, and litecoin) from the survey on the basis that they are unlikely to qualify as 'financial instruments'. Likewise, national financial authorities showed consensus around the suitability of excluding pure utility tokens from the perimeter of the existing financial regulation across member states on the basis that the rights they convey seem to be too far away from the financial and monetary structure of a transferable security and/or a financial instrument³⁹. This reasoning seems to also be in line with the characterization made by the Court of Justice of the European Union ("CJEU") analysed the concept of a chargeable event for VAT purposes in the context of payment tokens, specifically bitcoin⁴⁰. The court held that if the only purpose of possessing the digital tokens is to reuse them as a means of payment, for VAT purposes they must be treated in the same way as a legal tender if the activity on an exchange includes supply of services as per the VAT Directive⁴¹. This consequently might exclude them from the definition of transferable securities.

37 ESMA Report, p.5.

38 *Ibidem*.

39 *Ibid.*, p. 20.

40 C-264/14, Skatteverket v David Hedqvist, 2015, retrieved from <http://curia.europa.eu/juris/liste.jsf?num=C-264/14&language=EN>.

41 Value added tax directive (2006/112/EC).

From a practical perspective, the case-by-case basis approach undertaken by EU financial authorities in the context of Securities tokens adds to uncertainty, especially in relation to hybrid tokens, where investment-related features are combined with payment or utility features. The question to be answered is whether the financial instrument features prevail and how that will affect practicalities of conducting business activities. A lot of questions still remain to be answered, including whether authorisation requirements under MiFID2 should be applied to the DLT environment. The EACB sees MiFID2 as technology agnostic/ neutral and agrees that MiFID may apply in this context⁴². This, however, remains to be established by the EC, given the trading venue definitions relating to operations and authorisation of such venues to the very complex DLT environment.

Most recently, the French financial authority, *Autorité des Marchés Financiers* (“AMF”), proposed creating a “Digital Lab” at the European level to test Securities token projects with ESMA as the coordinator for digital tokens, acting in a supervisory role for digital tokens that do not qualify as financial instruments⁴³.

2. Legal framework potentially applicable to Securities tokens

Where digital tokens qualify as transferable securities or other types of financial instruments under MiFID2, a comprehensive set of EU financial rules, including the PR, the Transparency Directive, MiFID2, the Market Abuse Directive, the Short Selling Regulation and others are likely to apply to their issuer and/or firms providing investment services/activities to those instruments⁴⁴. Activities concerning Securities tokens would qualify as investment services/activities and transactions in Securities tokens admitted to trading or traded on a trading venue would be captured by various financial provisions discussed below⁴⁵.

42 EACB Response, p.36.

43 AMF (2020). Crypto-asset markets: the AMF responds to the European Commission consultation. Retrieved from: <https://www.amf-france.org/sites/default/files/pdf/62313/en/Crypto-asset%20markets%20the%20AMF%20responds%20to%20the%20European%20Commission%20consultation.pdf?1586938348>.

44 ESMA Report, p.5.

45 EC Consultation, p. 29.

Chart 2. – Overview of the financial EU rule set potentially applicable to digital tokens

EU legislative instrument	Area of relevance to digital tokens	Applicability
<p>MiFID2 and Markets in Financial Instruments Regulation (600/2014/EU) (“MiFIR”) (MiFID collectively)</p>	<p>Financial instruments</p>	<ul style="list-style-type: none"> » Definition considerations and whether digital tokens fall within scope of financial instruments under MiFID (Section C Annex 1 MiFID). » Whether hybrid assets with combined payment, utility, or investment features qualify as financial instruments <i>vis a vis</i> weight of their prevailing feature.
	<p>Investment firms, activities, and trading venues</p>	<ul style="list-style-type: none"> » Authorisation requirements for investment firms in a DLT environment. » Investment services and activities as per MiFID2 Article 4(1) and Section A of Annex 1 and applicability for Securities tokens. » Trading venue definitions (‘regulated market’, MTF, and OTF), operation, and authorisation requirements and applicability in DLT environment. » Access to trading venue under Article 53(3) and 19(2) of MiFID2 prevents retail clients from accessing trading venues <i>vis a vis</i> digital tokens users accessing trading platforms without an intermediary.
	<p>Investment protection, trade transparency, and transaction reporting</p>	<ul style="list-style-type: none"> » Investment protection rules covering information, documentation, and suitability assessment in the context of acting in the best interest of a client (Articles 24 and 25 of MiFID) and current marketing of digital tokens. » Pre- and post-trade transparency requirements under MiFIR within the context of thresholds specified in MiFID and availability of digital tokens data. » Transaction reporting obligations to maintain records and related data considerations.
	<p>Electronic trading and system resilience</p>	<ul style="list-style-type: none"> » MiFID requirements on effective systems and procedures resulting in resilient trading environment. » Direct electronic access for authorised investment firms or credit institutions.

Market Abuse Regulation (596/2014/EU) (“MAR”)	Market Manipulation	<ul style="list-style-type: none"> » Novel types of market manipulation may arise under Article 12(1)(a) of MAR defining that concept. This is due to differences in how Securities tokens are traded. » Value of financial instruments covered by MAR can be affected by trading manipulations in digital tokens.
	Insider Dealing	<ul style="list-style-type: none"> » Miners or wallet providers may hold insider information which can be used to commit market abuse. » Article 8(4) MAR contains a catch-all provision for insider dealing applicable to all persons with insider information.
Transparency Directive (2013/50/EU)	Disclosure requirements	<ul style="list-style-type: none"> » Issuers whose Securities tokens were admitted to trading on a regulated market situated or operating within an EU member state would have to disclose periodic and ongoing information.
Prospectus Regulation (2017/1129/EU) (“PR”)	Public offers	<ul style="list-style-type: none"> » Offer of securities to the public definition under Article 2(d) of the PR and coverage of digital tokens. » Applicability of prospectus exemptions for public offers (Article 1(4) PR) and admission to trading on a regulated market (Article 1(5) PR) and Securities tokens considerations.
	Schedules	<ul style="list-style-type: none"> » Format and content requirements of prospectus documents as per Delegated Regulation (EU) 2019/980 and specifics of Securities tokens.
	LEIs	<ul style="list-style-type: none"> » Securities tokens obtaining legal entity identifiers (“LEIs”) and International Securities Identification Number (“ISINs”).
	Risks	<ul style="list-style-type: none"> » Content of prospectus has to disclose material risks associated with the issuer of the security as per Article 16 of PR <i>vis a vis</i> digital token risks relating to cyber security, IT infrastructure, and technology.
Short Selling Regulation (236/2012/EU) (“SSR”)	Net short positions	<ul style="list-style-type: none"> » In a scenario when a position in a Securities token would provide financial advantage as a result of a decrease in value or price, SSR could be applicable. » This depends on the list of financial instruments set out in Annex 1 of Commission Delegated Regulations (EU) 98/2012.
Central Securities Depositories Regulation (909/2014/EU)	Book entry recording	<ul style="list-style-type: none"> » Article 3(2) of CSDR requires transferrable securities traded as part of MiFID 2 to be recorded in a book entry form in CSD. » National laws could pose restrictions on DLT in that context.
Settlement Finality Directive (98/26/EC) (“SFD”)	List of authorised persons	<ul style="list-style-type: none"> » List of persons authorised to participate in securities settlement system under SFD (investment firms, clearing houses, CCPs, etc.) does not include natural persons. » SFD conflict of laws could be seen as problematic.

European Markets Infrastructure Regulation (648/2012/EU)	Central clearing	<ul style="list-style-type: none"> » Central clearing obligations applicable to OTC derivatives may capture digital tokens with similar features of derivatives. » Additionally, MiFIR may capture exchange-traded derivatives in that context.
Financial Collateral Directive (2002/47/EC)	Collateral and title transfer	<ul style="list-style-type: none"> » Collateral that is provided without title transfer in the form of a pledge or other form of security needs to be enforceable in a distributed ledger. » The question of conflict of laws relating to security may pose challenges in that context.
Alternative Investment Fund Management Directive (2011/61/EU) (“AIFMD”)	Other assets’ applicability	<ul style="list-style-type: none"> » Those digital tokens that do not fall as financial instruments the rules for other assets under AIFMD may apply. » Safekeeping (verification of ownership and up-to-date record keeping) needs to be done by the depository.
Undertaking for Collective Investment in Transferable Securities Directive (2009/65/EC) (“UCITS”)	UCITS considerations	<ul style="list-style-type: none"> » Asset eligibility in conjunction with the meaning of financial instruments. » Arrangements for management, identification, and monitoring of conflict of interest. » Asset valuation calculation of issue price and repurchase price. » Appointment of depository and safekeeping considerations. » Disclosure and reporting requirements.
Capital Requirements Directive (2013/36/EU) and Capital Requirements Regulation (2013/575/EU)	Minimum capital requirements	<ul style="list-style-type: none"> » Minimum capital requirements to be complied with by digital token service providers where they potentially qualify as trading venues.

Source: EC Consultation and ESMA Report.

3. Practical considerations for service providers

3.1 Offering of Securities tokens

The PR requires publication of a prospectus before the offer of securities to the public in EU member states unless certain exclusions or exemptions apply. An offer of securities to the public as defined in the PR is a communication to persons in any form and by any means, presenting sufficient information on the terms of the offer and the securities to be offered, so as to enable an investor to decide to purchase or subscribe those securities⁴⁶. This definition also applies to the placement of securities through financial intermediaries.

The PR specifies that the prospectus shall contain the necessary information which is material to an investor for making an informed assessment of the financial condition of the issuer and of any guarantor, the rights attaching to the securities, and the reasons for the issuance and its impact on the issuer. The information shall be written and presented

⁴⁶ PR, Article 2 (d).

in an easily analysable and comprehensible form. The PR does not directly specify who should draw up the prospectus but requires the party responsible for the information (being at least the issuer or offeror) to be specified in the prospectus. The prospectus cannot be published until it has been approved by its EU national financial authority.

The definition of “*offer of securities to the public*” above is broad enough to encompass offers (e.g., Securities Token Offerings (“STOs”), ICOs, and Initial Exchange Offerings) and advertisement relating to digital tokens that could qualify as transferable securities under MiFID2. If these tokens are offered to the public, a prospectus would be required unless one of the exemptions for offers to the public under the PR applies.

The PR will not apply to those digital tokens that do not qualify as transferable securities, which may suggest that disclosure requirements for other financial instruments will depend on national law. In addition, the publication of bid and offer prices is not to be regarded in itself as an offer of securities to the public and is therefore not subject to the obligation to draw up a prospectus under the PR. In this last case, a prospectus should only be required where the publication is accompanied by a communication constituting an offer of securities to the public, under the terms discussed above⁴⁷.

There are a number of exemptions to the obligation of publishing a prospectus, based on different factors. Because of their relevance, it is worth mentioning those exemptions concerning the size of the offer and those related to the type of investor to which the offer is addressed:

Regarding the size of the offer, the requirement for the publication of a prospectus may not be triggered in several cases:

- » Offers below EUR 1M of total consideration in the EU as calculated over 12 months are exempt from the obligation to publish a prospectus.
- » Member states may decide to exempt offers below EUR 8M of total consideration in the EU as calculated over 12 months.
- » Between EUR 1M and EUR 8M, member states will select a threshold (not higher than EUR 8M) under which national requirements apply.

National requirements vary by member state.

Offers would also be exempt from the obligation if:

- » The offer is addressed only to qualified investors, which are essentially professional clients under MiFID2⁴⁸;
- » the offer is addressed to fewer than 150 natural or legal persons per member state other than qualified investors;

⁴⁷ PR, Recital 14.

⁴⁸ A professional client is a client who possesses the experience, knowledge, and expertise to make her/his own investment decisions and properly assess the risks that it incurs. In order to be considered to be professional client, the client must comply with the criteria established in Annex II of MiFID2.

- » the denomination per unit amounts to at least EUR 100,000; or
- » the offer is addressed to investors who acquire securities for a total consideration of at least EUR 100,000 per investor, for each separate offer.

Chart 3. – approaches taken by member states and their EU national financial authorities to the concept of transferable securities and prospectus requirements.

Country	Are digital tokens considered a security by financial authorities?	Prospectus needed ⁴⁹ ?
Austria	<p>Yes, when the design of the token is similar to “classical securities”, in particular bonds or shares, for instance, when the tokens:</p> <ul style="list-style-type: none"> » embody claims for a pay-out (“future cashflow”) towards the issuer; » provide rights under company law, such as voting rights at a general meeting; or » embody claims to the payment of capital, whether in the form of participation in the profits of the company or in the form of interest payments and repayment, regardless for such claims to exist in a legal tender ⁵⁰. 	<p>Yes, unless the exemptions in the PR apply or the offer’s total consideration in the EU is less than EUR 5 million.</p>
France	<p>Yes, if tokens can be classified as equity securities, debt securities, or as units or shares of collective investment undertakings. In a Discussion Paper published in 2017, the French financial authority noted that the tokens issued in France of which the authority was aware to that date did not fall under French regulations governing the public offering of financial securities⁵¹.</p>	<p>Yes, unless the exemptions in the PR apply or the offer:</p> <ul style="list-style-type: none"> » has a total consideration of less than EUR 8 million; or » is issued by credit institutions on a regular basis and have a value of less than EUR 75 million across the EU.

49 ESMA (2020). National thresholds below which the obligation to publish a prospectus does not apply. Retrieved from: https://www.esma.europa.eu/sites/default/files/library/esma31-62-1193_prospectus_thresholds.pdf.

50 FMA. Fintech navigator: ICOs. Retrieved from: <https://www.fma.gv.at/en/fintech-point-of-contact-sandbox/fintech-navigator/initial-coin-offerings/>.

51 AMF (2017). Discussion paper on initial coin offerings. Retrieved from: https://www.amf-france.org/sites/default/files/contentu_simple/consultations_publicques/AMF%20public%20consultation%20on%20Initial%20Coin%20Offerings%20%28ICOs%29.pdf, p. 7, 8.

<p>Germany</p>	<p>Yes, if tokens are:</p> <ul style="list-style-type: none"> » transferable, which is the case for the vast majority of the token standards existing on the market; » negotiable on financial markets, <i>i.e.</i>, they have a minimum level of standardization and are comparable to each other in the sense of a “class”; and » they convey rights similar to securities, <i>e.g.</i>, investment or membership rights⁵². 	<p>Yes, unless the exemptions in the PR apply or the offer’s total consideration in the EU is less than EUR 8 million.</p>
<p>Netherlands</p>	<p>Yes, if tokens are:</p> <ul style="list-style-type: none"> » transferable and negotiable on the financial markets; and » represent either (i) a share or equivalent right or instrument, (ii) a bond or other debt instrument, or (iii) any other instrument that can be converted into a share, bond or equivalent or that can be settled in cash. <p>Notably, the definition of security under Dutch law lists the three categories above as a closed, exhaustive list, in contrast to the MiFID2 definition which uses a non-exhaustive list, thus remaining open to other type of securities. As a result, the Dutch financial authority’s ability to interpret the term is significantly restricted in comparison to other member states in the EU⁵³.</p>	<p>Yes, unless the exemptions in the PR apply or the offer’s total consideration in the EU is less than EUR 5 million.</p>
<p>Spain</p>	<p>Yes, in case the token assigns rights or expectations to participate in:</p> <ul style="list-style-type: none"> » the potential increase in value of the token; or » in the profits generated by a project or business. <p>Also, utility tokens could qualify as financial instruments if they are sold appealing directly or indirectly to the buyer’s expectation to obtain profit from a value increase or some compensation linked to the token or mentioning the token’s liquidity or aptitude to be negotiated in markets that are similar or pretend to be similar to financial markets⁵⁴.</p>	<p>Yes, unless the exemptions in the PR apply or the offer’s total consideration in the EU is less than EUR 5 million.</p>

52 BaFin (2019). Guidance Notice on crypto tokens. Retrieved from: https://www.bafin.de/SharedDocs/Downloads/EN/Merkblatt/WA/dl_wa_merkblatt_ICOs_en.html;jsessionid=C7B411F6AB1B3A728F7F0C4A4E57A9E4.2_cid393, p.7.

53 AFM (2018). Cryptos: recommendations for a regulatory framework. Retrieved from: <https://www.afm.nl/en/nieuws/2019/jan/adviesrapport-crypto>, p.27.

54 CNMV (2018). Criterios en relación con las ICOs. Retrieved from: <http://cnmv.es/porta/verDoc.axd?t=%7b9c76eef8-839a-4c19-937f->

<p>United Kingdom⁵⁵</p>	<p>Yes, if there are factors indicating the token functions as a security, e.g., the contractual rights and obligations the token-holder has by virtue of holding or owning that token; any contractual entitlement to profit-share (like dividends), revenues, or other payment or benefit of any kind; any contractual entitlement to ownership in, or control of, the token issuer or other relevant person (like voting rights); the language used in relevant documentation, like token “whitepapers”, that suggests the tokens are intended to function as an investment⁵⁶.</p>	<p>Yes, unless the exemptions in the PR apply or the offer’s total consideration in the EU is less than EUR 8 million.</p>
---	--	--

Sources: the information displayed in the chart comes from documents released by financial authorities in the EU. Please consult the footnotes for further reference.

It is worth noting that in its response to the EC Consultation, EACB noted that exemptions included in the PR for offers to the public or to trading on a regulated market, should apply to Securities tokens without an additional or different approach. EACB also highlighted that the format and content of all prospectuses and their related documentation should not include specific schedules about Securities tokens and the principle of “*same business, same risk, same rules*” should apply⁵⁷.

3.2 Secondary market trading: admission to trading

The PR requires publication of a prospectus before securities may be traded on a regulated market situated or operating within a member state unless certain exclusions or exemptions apply. As with the offer of securities, the PR does not directly specify who should draw up the prospectus but requires that the party responsible for the information (being at least the party seeking admission to trading or guarantor) is specified in the prospectus. The prospectus cannot be published until it has been approved by the supervising EU national financial authority.

In addition, issuers whose securities are admitted to trading on a regulated market situated or operating within a member state shall disclose periodic and ongoing information under the Transparency Directive (“TD”)⁵⁸ about these issuers, e.g., annual financial reports, semi-annual reports, interim management statements, acquisition, or disposal of major holdings and any changes in the rights of securities holders. TD applies only where instruments are transferable securities, as defined in MiFID2.

Note that the PR and the TD require publication and disclosure when the admission

cfde6443e4bc%7d and updated by <http://cnmv.es/DocPortal/Fintech/CriteriosICOs.pdf>, pp. 2-3.

55 FCA (2019). Guidance on Cryptoassets. Consultation Paper (CP19/3). Retrieved from: <https://www.fca.org.uk/publication/consultation/cp19-03.pdf>, p.20.

56 FCA (2019). Guidance on Cryptoassets. Consultation Paper (CP19/3). Retrieved from: <https://www.fca.org.uk/publication/consultation/cp19-03.pdf>, p.20.

57 EACB Response, 43.

58 Transparency Directive (2013/50/EU).

relates to a regulated market⁵⁹. Accordingly, the mere admission of securities to trading on a Multilateral Trading Facility (“MTF”)⁶⁰ would in principle fall outside the perimeter of both the PR and the TD, and therefore would not be subject to the obligation to draw up a prospectus or to disclose information⁶¹.

3.3 Secondary market trading: trading platforms

3.3.1 General approach

As noted by the ECB, trading platforms are the gatekeepers that participate in networks where digital tokens transactions are instructed, and are validated to hold, buy, and sell those assets on behalf of their clients⁶². The current regulatory approach to digital token platforms requires a change because their decentralised gatekeeping activities and associated risks may be amplified by trading platforms’ existing operational models, as is pointed out by the G7 in a paper on “stablecoins” (“G7 Report”⁶³).

Trading platforms can have different legal qualifications depending on the way they operate. Where these platforms qualify as trading venues (as regulated markets, MTFs or Organised Trading Facilities (“OTFs”)⁶⁴) as defined in MiFID2, they will fall under the scope of the directive and must comply with the different rules and requirements set therein, including obtaining authorisation. According to ESMA⁶⁵, the relevant aspects to determine whether a trading platform shall be considered a trading venue under MiFID2 are the following:

- » Where digital tokens qualify as financial instruments, platforms trading digital tokens with a central order book and/or matching orders under other trading models are likely to qualify as multilateral systems⁶⁶ and should therefore either operate under the rules set forth in MiFID2 as regulated markets, MTFs, or OTFs.
- » Where the operators of those platforms are dealing on their own account and executing client orders against their proprietary capital, they would not qualify as multilateral trading venues but rather as broker/dealers providing services that fall under MiFID2 and should therefore comply with the requirements set

59 Regulated market means a multilateral system operated and/or managed by a market operator, which brings together or facilitates the bringing together of multiple third-party buying and selling interests in financial instruments – in the system and in accordance with its non-discretionary rules – in a way that results in a contract, in respect of the financial instruments admitted to trading under its rules and/or systems, and which is authorised and functions regularly and in accordance with Title III of MiFID2.

60 Multilateral trading facility or MTF means a multilateral system, operated by an investment firm or a market operator, which brings together multiple third-party buying and selling interests in financial instruments – in the system and in accordance with non-discretionary rules – in a way that results in a contract in accordance with Title II of MiFID2.

61 PR, Recital 14.

62 ECB Report, p.30.

63 G7 Working Group on Stablecoins. (2019). Investigating the impact of global stablecoins. Retrieved from: <https://www.bis.org/cpmi/publ/d187.pdf>.

64 Organised trading facility or OTF means a multilateral system which is not a regulated market or an MTF and in which multiple third-party buying and selling interests in bonds, structured finance products, emission allowances or derivatives are able to interact in the system in a way that results in a contract in accordance with Title II of MiFID2.

65 ESMA Report, pp. 25-29.

66 Multilateral system means any system or facility in which multiple third-party buying and selling trading interests in financial instruments are able to interact in the system.

out in the directive.

- » Platforms that are used to advertise buying and selling interests where there is no genuine trade execution or arrangement taking place may be considered as “bulletin boards” and fall outside of the scope of MiFID2⁶⁷.

Challenges arise when trying to define the legal nature of hybrid platforms, *i.e.*, those trading platforms that include a combination of the features described above. For instance, a platform could match orders but not necessarily proceed to execute them, which instead can be managed through a smart contract. Whether these platforms would qualify as regulated markets, MTFs, OTFs, investment firms, or none of them is currently debatable and would therefore depend on the interpretation of policy makers and financial authorities in member states.

3.3.2 Practical considerations for trading venues

Based on the assessment above, platforms qualifying as trading venues or as broker/dealers will have to implement different rules and requirements established in applicable financial regulations, with special attention to the following, as discussed in the EC Consultation⁶⁸.

- » **Authorisation:** under MiFID2, trading venues shall be operated either by a market operator (‘regulated markets’) or an investment firm (MTF or OTF) and both market operators and investment firms must obtain authorisations to provide their services. Specific authorisations vary by member state, where some countries accept the authorisation as an investment firm to operate MTFs and OTFs and others have developed specific authorisations for each trading venue category.
- » **Capital requirements:** investment firms need to comply with the minimum capital requirements as set out in MiFID2 and Capital Requirements Directive and Capital Requirements Regulation (“CRD IV/CRR”). They vary depending on the type of MiFID2 services/activities carried out. For instance, investment firms operating an MTF or an OTF or dealing on their own account need to have an initial capital of EUR 730,000 minimum⁶⁹.
- » **Organizational requirements:** trading venues shall have in place effective systems, procedures, and arrangements to ensure its trading systems are resilient, keep sufficient capacity, and can respond adequately in case of system failure.
- » **Admission of financial instruments:** trading venues shall establish rules to ensure that financial instruments admitted to trading are capable of being

67 More on this analysis in: AMF (2020). Review and analysis of the application of financial regulations to security tokens. Retrieved from: https://www.amf-france.org/sites/default/files/2020-03/legal-analysis-security-tokens-amf-en_1.pdf, pp. 16-17.

68 EC Consultation, p.37.

69 ESMA Report, p. 25.

traded in a fair, orderly, and efficient manner.

- » **Access to trading venues:** trading venues may admit as members or participants only investment firms, credit institutions, and other persons with sufficient reputations with the aim of protecting investors and the proper functioning of financial markets. Where trading platforms allow the exchange of Securities tokens, these requirements may conflict with allowing retail investors to directly access the platform without any intermediation.
- » **Transparency and reporting:** under MiFIR⁷⁰, trading venues must follow pre-transparency and post-transparency requirements in relation to equity and non-equity. Investment firms must report transactions to their financial authority. These would apply when trading platforms operate with Securities tokens.
- » **Market abuse:** the MAR⁷¹ aims at protecting market integrity. Trading platforms, as well as other operators exchanging digital tokens such as miners or wallet providers, could be captured by this regulation when dealing with Securities tokens and would be subject to the corrective actions to market manipulation or fight against insider dealing.
- » **Settlement-related obligations:** if the digital tokens are transferable securities which are traded on a trading venue or transferred following a financial collateral arrangement, they would have to be recorded with an authorised central securities depository (“CSD”)⁷². An operator of a trading platform or a DLT network would therefore need to seek authorisation as a CSD or work with an authorised CSD and therefore assume the economic and logistic efforts derived from it⁷³.

However, as noted by the EC⁷⁴, there have been few instances of Securities tokens issuance (for example, the German Fundament STO authorised by the German financial authority, BaFin, in July 2019) with none of them actually admitted to trading. At the same time, in late 2018, the Austrian Financial Market Authority approved the capital market prospectus of Hydrominer IT-Services GmbH for public offering⁷⁵. As reported by the AMF, there were a few instances where STOs were issued in France, but the majority of them in accordance with French law were not classified as public offers and were not covered by the prospectus requirements⁷⁶.

70 Markets in Financial Instruments Regulation (600/2014/EU).

71 Market Abuse Regulation (596/2014/EU).

72 Central securities depository means a legal person that operates a securities settlement system (*i.e.*, a multilateral arrangement between three or more participants to standardize the rules for the execution and transfer of orders between participants) and providing at least one of the following core services: (i) initial recording of securities in a book-entry system ('notary service'); (ii) providing and maintaining securities accounts at the top tier level ('central maintenance service'); and (iii) operating a securities settlement system ('settlement service').

73 ESMA Report, p. 31.

74 EC Consultation, p. 29.

75 See <https://www.svlaw.at/en/stadler-voelkel-beraten-bei-erstem-security-token-offering-in-der-europaeischen-union-auf-basis-eines-kapitalmarktprospekts>.

76 See https://www.amf-france.org/sites/default/files/2020-03/legal-analysis-security-tokens-amf-en_1.pdf.

The EC Consultation underscores that, as a matter of principle, Securities tokens are already covered by the EU legal framework in relation to asset management via the scope of financial instruments under MiFID2 as discussed above. This does not exclude a potential gradual regulatory approach including legal certainty for centralised platforms first and decentralised platforms falling next in line⁷⁷. In its last response, EACB responded to a question from the EC on recent market developments in the context of Securities tokens with the following statement: *“In the past there have been many attempts to [engage in] fraudulent activities and/or factual avoidance of existing legislation. We are of the opinion that the more tokens [that] fall under legislation, the less the interest of issuers is”*⁷⁸. This highlights the need for a common approach that addresses when a Securities token constitutes a financial instrument.

C. DLT TRANSFERABLE SECURITIES

The Pilot Regime Proposal, Article 5, states that “DLT transferable securities” means transferable securities within the meaning of Article 4(1)(44) (a) and (b) of MIFID2 that are issued, recorded, transferred, and stored using DLT.

DLT transferable securities are, therefore, a specific subset of Securities tokens, which are limited to those matching the definition of transferable security under MIFID2. The Pilot Regime Proposal creates this token’s category to limit the type of financial instruments that could be admitted to trading in “DLT market infrastructures”⁷⁹. As we will explore below, only certain DLT transferable securities meeting some the conditions may be admitted to trading in these infrastructures.

D. EC PROPOSAL ON REGULATED TOKENS

The EC released two non-papers in May and July 2020 in which it went through a number of measures that might turn into a proposal to create a pan-EU regulatory framework for markets in digital tokens. It is worth noting that the views expressed in the non-papers may not in any circumstances be regarded as stating an official position of the EC, but they serve as working documents between the EC and the stakeholders involved in the initiative.

In relation to digital tokens falling within the EU financial regulatory framework, the EC understands that the issues seen throughout this section could be tackled through a combination of legislative and non-legislative measures. In particular, the EC indicates three options to consider:

- » Non-legislative measures which would provide guidance on how existing legislation applies to digital tokens;
- » Targeted legislative changes removing provisions acting as a barrier to issuance, trading, and

⁷⁷ EC Consultation, p.30.

⁷⁸ EACB Response, p.32.

⁷⁹ Article 2(2) of the Pilot Regime Proposal defines a DLT market infrastructure means either a “DLT multilateral trading facility” or a “DLT securities settlement system”, as defined in Articles 2(3) and (4) of the same Regulation.

post-trading of Securities tokens; and

- » A pilot regime for DLT market infrastructures for digital tokens that qualify as financial instruments.

1. Guidance on how existing legislation applies to crypto assets

The non-paper proposes an interpretative communication where the EC sets its view on the characteristics digital tokens should have to qualify as financial instruments or e-money under the EU financial services regulatory framework. As an additional action, the non-paper mentions that the EC could provide guidance on how existing sectoral legislation applies, according to the EC, to digital tokens that would qualify as “financial instruments” (such as MiFID2, the Prospectus Regulation, the Central Security Depository Regulation, and the Settlement Finality Directive)⁸⁰.

2. Potential targeted amendments to existing financial services legislation

Where provisions of sectoral legislation would clearly hinder or prevent the use of DLT or Securities tokens or where proper application of the legislation in a DLT environment cannot be assured, the EC may present targeted amendments to address these issues. These amendments might not require Level 1 changes (*i.e.*, changes to the law), but instead could require level 2 modifications (*i.e.*, technical implementing measures) and could also be done if and when the legislation in question is being reviewed⁸¹.

Those targeted changes would enable the use of centralised networks and permission-based DLT. Most notably, this initiative could include a targeted amendment to the notion of financial instruments under the MiFID2, to make sure that such an instrument can be issued on a DLT⁸².

3. Pilot Regime

In July’s version of the non-paper, the EC noted that there is a lack of market infrastructure in the DLT realm as legal uncertainty discourages the establishment of trading venues or CSDs⁸³. This infrastructure would enable the trading and settlement of digital tokens, would allow the development of secondary markets for Securities tokens to support the nascent primary markets and would help to create the conditions for these markets to scale.

To solve this issue, the EC has released the Pilot Regime Proposal, as part of their proposal for an EU framework on digital tokens.

The pilot regime would function as a temporary sandbox open for a period of up to six years, during which DLT market infrastructures could operate exempted from some specific

80 European Commission (EC). (2020), Non-paper on the legislative proposals for an EU framework for markets in crypto-assets. Retrieved from https://www.politico.eu/wp-content/uploads/2020/05/May-14_3.pdf, p.4.

81 *Ibid.*

82 European Commission (EC). (2020), Non-paper on the legislative proposals for an EU framework for markets in crypto-assets, July update. Retrieved from https://drive.google.com/file/d/1ZBI_YSUcKblJCrsOtoQk66z4jtd7Dvkj/view, p.1.

83 A central securities depository or CSD means a legal person that operates a securities settlement system referred, as defined in Article 2(1)(1) of Regulation (EU) No 909/2014.

requirements under the EU financial services legislation. The aim is to temporarily remove certain regulatory obstacles that could be preventing the development of DLT infrastructure, therefore enabling both market participants and regulators to gain experience and to explore the risks posed by this infrastructure.

A DLT market infrastructure would either function as a DLT MTF or a DLT CSD. Operators of these venues would be required to obtain an authorization by their local financial authority, on top of their existing authorisation as investment firm, market operator (in the case of DLT MTFs), or as a CSD (in the case of DLT CSDs).

During the time-limited experimentation, the DLT market infrastructure would only be allowed to admit to trading or to record on the ledger simple financial instruments (*i.e.*, shares and bonds) that are not liquid. In turn, the participants can apply for exemptions when operating, most notably the possibility to admit retail investors in their customer base, thus removing the obligation of intermediation through investment firms, credit institutions, and other persons with sufficient level of trading ability.

National financial authorities would have the power to impose corrective measures on the DLT market infrastructure and to withdraw the permission under some circumstances. ESMA would fulfil a coordination role between competent authorities.

The Proposal states that, after a five-year period from the entry into application of this Regulation, ESMA should report to the EC on this pilot regime for DLT market infrastructures, including on the potential benefits linked to the use of DLT, the risks raised, and the technical difficulties. Based on ESMA's report, the EC should report to the Council and European Parliament. This report should assess the costs and benefits of extending this regime on DLT market infrastructures for another period of time, extending this regime to new type of financial instruments, making this regime permanent with or without modifications, bringing modifications to the EU financial services legislation or terminating this regime.

IV. Digital Tokens Outside The EU Financial Regime

A. INTRODUCTION: PROPOSAL FOR A REGULATION ON MARKETS IN CRYPTO-ASSETS REGULATION

The ESMA Report raised concerns regarding the risk of consumer/investor lack of protection given that most digital tokens are not likely to qualify as financial instruments under MIFID2 and, therefore, are likely to fall outside the existing EU financial services rules⁸⁴. As a result, consumers and investors will not benefit from the safeguards provided by these rules while not being able to easily distinguish whether digital tokens available in the same trading venues are within the scope of the EU's financial legal framework. In addition, some EU member states have implemented or are considering bespoke regimes for digital tokens that do not qualify as financial instruments, with the notable example of the French PACTE law and Malta's three

84 85 European Securities and Markets Authority (ESMA). (2019). Advice Initial Coin Offerings and Crypto-Assets. Retrieved from <https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection>, p.5.

acts on DLTs⁸⁵, thus helping to foster regulatory fragmentation across the EU.

With that in mind, the EC Consultation also sought views to assess whether regulating the unregulated digital token space could be beneficial at this point. As a result, the MiCA Regulation Proposal proposes a bespoke regime to regulate digital tokens falling outside the perimeter of the financial services framework. It establishes harmonised requirements at the EU level for issuers that seek to offer their digital tokens across the EU and for “crypto-asset service providers” wishing to apply for an authorisation to render their services in the single market, where these digital tokens do not qualify as financial instruments. This initiative would replace existing national frameworks applicable to digital tokens not covered by existing EU financial services legislation.

B. CLASSIFICATION OF DIGITAL TOKENS IN THE MICA REGULATION PROPOSAL

The MiCA Regulation Proposal includes a wide definition of “crypto-asset”⁸⁶ with the intention of capturing all types of digital tokens which currently fall outside the scope of EU financial services legislation, thus ensuring that the MiCA Regulation Proposal is future-proof and keep pace with innovation and technology developments in the sector.

Beyond the general definition of crypto-assets, the MiCA Regulation Proposal distinguishes between three sub-categories of digital tokens that are be subject to specific requirements: “utility tokens”, “e-money tokens”, and “asset-referenced tokens”.

1. Utility tokens

According to the MiCA Regulation Proposal, utility token refers to “a type of crypto-assets which are intended to provide access digitally to an application, services or resources available on a distributed ledger and that are accepted only by the issuer of that token to grant access to such application, services or resources available”⁸⁷.

The fact that the MiCA Regulation Proposal decided to define this kind of asset as a specific sub-category and leave payment tokens undefined could be a good indicator to show that this Regulation excludes pure payment tokens from its scope. That would be the case if payment tokens do not qualify as e-money tokens or asset-referenced tokens. This entails that digital tokens such as bitcoin, litecoin, bitcoin cash or other projects which are not focused on stabilising the token’s value, are out of the scope of this Regulation Proposal.

85 In France, the PACTE law has created a specific framework for the offering of utility tokens to the public and to regulate certain aspects, such as safety and operational risks, internal control mechanisms, resilience of IT systems, and conflicts of interest, for different service providers dealing with crypto-assets that do not qualify as financial instruments under MIFID2. The regime is optional, meaning that service providers will not have to comply with its rules and requirements unless they decide to opt in, a point from which they will have to comply in full. In other words, this legal setup offers crypto-asset service providers a trade-off between legal certainty and compliance costs. This novel approach has been both praised and criticised, the latter’s most prominent voice being the ESMA, which although understands the intention to support these instruments, stresses that these kinds of initiatives do not help to provide for a homogeneous framework across the EU. In Malta, the Maltese legislator has adopted three acts relating to DLT, which entered into force on 1 November 2018: (i) the Virtual Financial Assets Act, (ii) the Malta Digital Innovation Authority Act, and (iii) the Innovative Technology Arrangement and Services Act. These three acts introduce, among other measures, a requirement for issuers of virtual financial assets to draw up and make available a white paper, licensing requirements for providers of virtual financial services such as brokers, conduct of business rules for license holders and certain AML requirements for license holders.

86 Crypto-asset is defined in the MiCA Regulation Proposal, Article 3(1)(2), as “a digital representation of value or rights, which may be transferred and stored electronically, using distributed ledger or similar technology”.

87 See Article 3(1)(5) of the Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1600947409472&uri=COM:2020:593:FIN>.

2. E-money tokens

According to the MiCA Regulation Proposal, an e-money token is a “type of crypto-assets whose main purpose is to be used as a means of exchange and that purports to maintain a stable value by being denominated in (units of) a fiat currency”⁸⁸. The Regulation Proposal determines that crypto-assets qualifying as e-money under EMD2 but not as e-money tokens under the MiCA Regulation Proposal, will be outside MiCA’s perimeter.

Despite their similarities, some differences exist between digital tokens qualifying as e-money under EMD2 and e-money tokens. For instance, holders of e-money under EMD2 are always provided with a claim against an e-money institution and have a contractual right to redeem their e-money against fiat currency at par value with the fiat currency and at any moment. By contrast, some e-money tokens do not provide their holders with such a claim on their issuers and could fall outside the scope of EMD2. In addition, other e-money tokens do not provide a claim at par with the fiat currency they are referencing or limit the redemption period.

The reason to create the legal institution of e-money tokens as opposed to digital tokens falling under the scope of EMD2 (as seen in Section III(A)), is to create a wide definition to capture all the types of digital tokens referencing one single fiat currency on the market to prevent regulatory arbitrage with the provisions of the EMD2 or the circumvention of EU rules⁸⁹.

Some stablecoins, depending on how they are structured, are 1:1 pegged to fiat currency, such as Tether, and could potentially fall under this category.

3. Asset-referenced tokens

Asset-referenced token means a “type of crypto-assets whose main purpose is to be used as a means of exchange and that purports to maintain a stable value by referring to the value of several fiat currencies, one or several commodities or one or several crypto-assets, or a combination of such assets”⁹⁰.

This category would apply to stablecoins which are not pegged to a fiat currency and, importantly, which do not qualify as financial instruments. Notably, the so-called algorithmic stablecoins that aim at maintaining a stable value, via protocols, that provide for the increase or decrease of the supply of such digital tokens in response to changes in demand should not be considered as asset-referenced tokens, provided that they do not aim at stabilising their value by referencing one or several other assets.

88 *Ibid.*, See Article 3(1)(4).

89 Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1600947409472&uri=COM:2020:593:FIN>, p. 16-17.

90 *Ibid.*, Article 3(1)(3).

C. REQUIREMENTS ON ISSUERS OF CRYPTO-ASSETS, ASSET-REFERENCED TOKENS, AND E-MONEY TOKENS

In relation to the issuance of crypto-assets, MiCA establishes requirements on issuers of:

- » crypto-assets (tokens outside the definition of a financial instrument, with utility tokens in mind);
- » asset-referenced or significant asset-referenced tokens; and
- » e-money tokens.

In relation to the issuance of crypto-assets, the MiCA Regulation Proposal mandates the publication of a harmonised whitepaper/information document with mandatory disclosures (detailed description of the issuer, the project and planned use of funds, conditions of the offer, rights, and obligations attached to the crypto-assets and risks). Small offerings (value under EUR 1 million within a twelve-month period) and offerings aimed at qualified investors as defined in the PR might be exempted from this requirement, as well as other cases listed in Article 4(2) of the Proposal. The whitepaper shall not be sanctioned by national financial authorities although it should be notified prior to its publication.

It will be the responsibility of the issuer to justify before national financial authorities why the digital token in question does not qualify as a financial instrument or as a deposit under MIFID2 or as e-money under EMD2.

Issuers of asset-referenced tokens will have to obtain authorisation before conducting an offering unless the average standing amount of asset-referenced tokens does not exceed EUR 5,000,000 over a period of 12 months, or the offer is addressed to qualified investors only. Issuers of these tokens will also have to comply with a number of requirements, for instance to be established as an EU legal entity, to disclose the rights attached to the asset-referenced token, including any potential direct claim on the issuer or the reserve of assets, and be required to publish a whitepaper with additional mandatory disclosures to those mandated in the case of regular issuances. Further, the whitepaper will have to be approved by national financial authorities (unless the offer did not need to be subject to authorization, in which case the whitepaper would only need to be notified), which will be in charge of the authorisation and ongoing supervision of issuers of asset-referenced tokens.

As for the issuers of e-money tokens, the MiCA Regulation Proposal imposes the obligation for these e-money tokens to be issued either by a credit institution authorised under Regulation (EU) 2013/575 or by an electronic money institution under EMD2. It is worth noting that they shall grant their users with a claim at any moment and at par value with the fiat currency referenced.

D. SERVICE PROVIDERS SUBJECT TO AUTHORIZATION

In relation to “crypto-asset service providers”, the MiCA Regulation Proposal would regulate the following services:

- » Custody and administration of crypto-assets on behalf of third parties;
- » Operation of a trading platform for crypto-assets;
- » Exchange of crypto-assets for fiat currency;

- » Exchange of crypto-assets for other crypto-assets;
- » Reception and transmission of orders for crypto-assets on behalf of third parties;
- » Execution of orders for crypto-assets on behalf of third parties;
- » Placing of crypto-assets;
- » Advice on crypto-assets; and
- » Payment transactions in asset-referenced tokens.

ESMA shall establish a register of all crypto-asset service providers. That register shall be publicly available on its website and shall be updated on a regular basis.

National financial authorities are envisaged to be in charge of the authorisation of the crypto-asset service providers. Once authorised, they would be allowed to provide their services across the Union.

Each type of provider would be subject to a number of specific rules⁹¹, depending on the type of service concerned, and all of them would need to comply with a set of general rules regarding good faith, prudential requirements on capital, organisational requirements about their personnel and management, information to competent authorities, safekeeping of funds, complaints procedures, conflict of interest, and outsourcing requirements.

E. SPECIFIC CONSIDERATIONS REGARDING STABLECOINS

1. Legal qualification of stablecoins

Although the MiCA Regulation Proposal has sought to create a uniform framework for some types of stablecoins, *i.e.*, e-money tokens and asset-referenced tokens, relevant complexities remain when trying to fit stablecoins in existing/proposed legal institutions, including all the above mentioned (financial instruments, e-money token an asset-referenced token). Some of those digital tokens may qualify as e-money under EMD2 or a financial instrument under MiFID2 due to the nature of the underlying asset, whereas others may fall outside of the current EU financial regime.

For instance, in its response to the EC Consultation, the European Association of Cooperative Banks responded that *“it is absolutely unclear what they are for the time being”*, potentially being from just a “marketing label”, e-money or some kind of tokenised money market fund with assets kept at a custodian/depositary⁹².

Other stakeholders have stated that crypto-assets with commodities as underlying assets share the same characteristics as commodity derivatives, for instance, the SMSG⁹³. ESMA categorised stablecoins as similar to securities with reference to transferable commodities, and, therefore,

⁹¹ For more information please consult Articles 67 to 73 of the MiCA Regulation Proposal.

⁹² See p. 58 in EACB’s response to the EC Consultation in the link provided in footnote 46.

⁹³ Securities and Markets Stakeholder Group (SMSG). (2018), Advice to ESMA: Own Initiative Report on Initial Coin Offerings and Crypto-Assets. Retrieved from: https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf, p. 11.

potentially part of the definition of “transferrable securities” under MIFID2⁹⁴. Further, in October 2019, the G7 published a paper on stablecoins⁹⁵ which seems to follow a similar approach to ESMA.

2. Practical considerations

Legal certainty in this field is still to be developed within the EU given the relatively new nature of stablecoins. Legal classification has attracted a lot of attention both within the markets and across relevant EU national financial authorities. The underlying technicalities and contractual arrangements that are part of stablecoins may vary and the legal regimes applicable will depend crucially on the specific design of those digital tokens. Currently, digital token markets recognise asset-backed, crypto-collateralised, and algorithmic stablecoins⁹⁶. A non-exhaustive list of example design/business models currently used on the financial market includes:

- » Users have a direct claim on the issuer or the underlying assets that is often liquid and the provider pledges to redeem coins at par value in the same currency that was used to purchase the coins. This specific design would potentially qualify as e-money token under the conditions set in the MiCA Regulation Proposal.
- » The coin is backed by a claim against the issuer for fiat, which may involve a regulated bank with deposit insurance for trust enhancement.
- » The coin is not issued with specific face value but forms part of a portfolio of underlying assets similar to exchange-traded funds (“ETF”). This specific design would potentially qualify as an asset-referenced token or as a Securities token, depending on the case.

Within the context of the above design models, financial institutions may provide custodian or wallet services that are subject to existing international standards. In fact, the Financial Action Task Force (“FATF”) released a recommendation that relates to transfers of digital tokens to fiat currencies that banks may rely upon⁹⁷. With that in mind, the Basel Committee on Banking Supervision (“BCBS”) has set out prudential expectations regarding banks with exposure to digital tokens including due diligence, clear and robust risk management, and disclosure requirements⁹⁸. The more complicated situation, however, may arise with new entities and their business models where authorities have no legal tools to respond, potentially leading to reserve

94 European Securities and Markets Authority (ESMA). (2019). Advice Initial Coin Offerings and Crypto-Assets. Retrieved from <https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection>, p.19.

95 G7 Working Group on Stablecoins. (2019), Investigating the impact of global stablecoins. Retrieved from: <https://www.bis.org/cpmi/publ/d187.pdf>.

96 In the asset-backed sphere of stablecoins, those digital tokens are currently backed by either USD, EUR, or Chinese Yuan, this is a non-exhaustive list as other include stablecoins backed by gold or even Swiss commercial real estate. Tether dominates the stablecoin market with 90% of traded volumes and market cap of USD 32 bn (dated as of February 15). The crypto-collateralised stablecoins are backed on-chain with another digital token with a floating peg to 1 USD, whereas the algorithmic stablecoins peak cap USD 674m failed to recover after a drop in March 2018 according to Coinbase, a digital token exchange.

97 FAFT (2015). Guidance for a risk-based approach: virtual currencies. Retrieve from: <https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>.

98 Basel Committee on Banking Supervision (2020). Discussion paper: designing a prudential treatment for crypto-assets. Retrieved from: <https://www.bis.org/bcb/publ/d490.pdf>.

pools treated as a collective investment vehicle. This of course does not exclude the possibility of classification as securities (FCAs suggestion) or e-money (ECB consideration) built upon arguments in relation to functionalities of those digital tokens.

V. Other Relevant Legal Considerations For Digital Tokens: Tax Considerations

A. BLOCKCHAIN, DIGITAL TOKENS, AND TAXATION OF TOKENS

Since the emergence of bitcoin and other digital tokens, the taxation of digital tokens has been an important topic considered by regulators and tax authorities but also for holders of these digital tokens. Not surprisingly, from a regulatory and taxation perspective, the focus has been on the risks involved with these assets, such as money laundering, cybercrime, and tax evasion. In many EU countries, these risks have led to increased interest from policy makers, regulatory bodies, and tax authorities. Also, the OECD has recently issued a report called “Taxing Virtual Currencies: An Overview Of Tax Treatments And Emerging Tax Policy Issues” in which the tax aspects and policy considerations of digital tokens in some 50 countries have been addressed⁹⁹.

As is common with new business models and other developments, whether it is e-commerce or emerging technologies, many questions from a regulatory, policy, and taxation perspective arise. For technologies that are as nascent as blockchain and other DLT, this holds true even more. Even though the technology is now over a decade old, the number of people that fully (or partially) understand the technology remains limited. This is visible in both private and public organizations and can be seen as an impediment for clear and consistent policy and legislation on this topic. Slowly but gradually many EU countries are ramping up the number of people involved with digital tokens at tax authorities and financial law enforcement agencies.

There is a clear and desired role for EU organizations such as the EU Blockchain Observatory & Forum and other supranational organizations such as the Organisation for Economic Co-operation and Development (“OECD”) Global Blockchain Policy Centre to provide guidance and policy standards for governments. Harmonisation of standards, nomenclature, and policy guidelines is required in order to prevent EU countries from either reinventing the wheel or creating diverging rules and regulations that may lead to double taxation or non-taxation.

The token economy has transformed from a somewhat anarchistic movement to one of the larger classes of investments. According to coinmarketcap.com, a well-known site on market prices for digital tokens, over 5,300 digital tokens existed at the start of 2020, with a total market capitalization exceeding USD 250 billion¹⁰⁰. Due to the fact that digital tokens do not have a uniform definition, nor content, they are subjected to different tax regimes in different jurisdictions.

99 OECD (2020), Taxing Virtual Currencies: An Overview Of Tax Treatments And Emerging Tax Policy Issues, OECD, Paris. www.oecd.org/tax-policy/taxing-virtual-currencies-an-overview-of-tax-treatments-and-emerging-tax-policy-issues.htm.

100 R. Houben and A. Snyers (2020). Crypto-assets Key developments, regulatory concerns and responses (report requested by the European Parliament), p. 13.

From a tax perspective, it is worth making a distinction between the following types of tokens: currencies, assets, utility, and securities. Jurisdictions within the EU apply different tax regimes to the four categories, although there is a lot of unclarity still around the taxation of other tokens than currencies. Furthermore, from a tax perspective, how a person uses the tokens is assessed differently, *i.e.*, whether they are bought as an investment, used for payment purposes, or received as payment for services or as a gift/inheritance etc.

Coupling the characteristics of a token with the user's stated intention for the usage of the token provides an initial framework for domestic taxation of the tokens. This leaves us with a two-part assessment, where the extent to which the value of tokens would be seen as a taxable event stems from 1) assessing their characteristics, differentiated between (a) cryptocurrency, (b) virtual asset, or (c) security, coupled with 2) assessing the intention of the token-holder differentiated between (d) holding/investment, (e) transaction/payments, or (f) recipient of tokens as payment for services, gift/inheritance. From this two-part test, a number of tax-related questions arise in terms of the valuation of the tokens, timing of taxation, and beneficial ownership of the tokens.

Another area that raises tax-related queries is decentralised finance ("DeFi"). This is a fast-growing novel concept that can be described as building conventional financial services and products, such as lending, borrowing, exchange, derivatives etc., on a blockchain. Hence, it is a smart contract that governs and executes the financial service or product. We will look into some fundamental issues regarding locking up digital tokens into a DeFi smart contract, while generating a new token.

Notwithstanding the aforementioned risks, uncertainties, and lack of clarity regarding the taxation of different types of tokens, another important angle from a taxation perspective is the compelling combination of blockchain and tax, particularly as it pertains to immutability. For example, how smart contracts can arrange for immediate payments to tax authorities, has led to initiatives from private and public organizations to create more robust tax systems using blockchain technology, such as in the area of VAT. It is therefore also important to assess some of the possibilities and existing initiatives that can be seen in this area.

This chapter on taxation is built up as follows. In the next section, we delve into the potential for blockchain technology to create more robust tax systems at both an EU and at an EU member state level and describe some of the developments and potential future perspectives. After that, we will explore some of the general principles relevant to the taxation of digital tokens, such as mining and airdrops. We will also discuss the example of DeFi and the tax questions surrounding that use case. We will end with a section on the potential path forward and what is required to create more certainty and clarity around the taxation of digital tokens.

B. EU AND TAXATION: HOW TO USE BLOCKCHAIN TO CREATE MORE ROBUST TAX SYSTEMS

1. General comments

The EC is taking a holistic approach to blockchain and DLT¹⁰¹. For this, the EU relies on several initiatives to enable globally inclusive governance, reinforce cooperation and investments in deploying blockchain/DL- based applications, support international standard setting, and facilitate dialogue between industry stakeholders and regulators, notably for a regulatory framework, that builds on the EU acquis. As a follow-up from the Commission's FinTech Action Plan from 2018¹⁰², the Commission is working towards deepening the Single Market for digital financial services, promoting a data-driven financial sector in the EU while addressing its risks, and ensuring a level playing field, making the EU financial services regulatory framework more innovation-friendly, and enhancing the digital operational resilience of the financial system¹⁰³. In this section, we will highlight some of these initiatives as they may impact the way the EU will approach taxation as well.

The European Blockchain Partnership, which was created in April 2018, includes all EU member states and members of the European Economic Area (Norway and Liechtenstein). The aim is to work together towards realizing the potential of blockchain-based services for the benefit of citizens, society, and the economy. As part of this commitment, the Partnership is building a European Blockchain Services Infrastructure ("EBSI"). From its website¹⁰⁴ it can be derived that the EBSI will be materialized as a network of distributed nodes across Europe (the blockchain), leveraging an increasing number of applications focused on specific use cases. It is expected that EBSI will become a Connecting European Facility Building Block, providing reusable software, specifications, and services to support adoption by EU institutions and European public administrations.

Although one may argue whether it is most efficient or effective that a separate EBSI blockchain platform is being built as opposed to using existing blockchain platforms (e.g., the 100% open source Ethereum platform), it may be expected that EBSI will provide for standardization at an EU level when it comes to implementation of blockchain technology for regulatory and legislative purposes. That said, for taxation purposes the platform may be used in several areas. These areas may include, but are not limited to:

» Exchange of information regarding taxpayers on:

- exchange of tax rulings;
- multi-country tax audits;
- country-by-country reporting.

¹⁰¹ See for more on the EU strategy <https://ec.europa.eu/digital-single-market/en/blockchain-technologies>.

¹⁰² Commission's Communication: FinTech Action Plan: For a more competitive and innovative European financial sector (March 2018).

¹⁰³ EC Consultation, p. 3.

¹⁰⁴ EBSI. Experience the future with the European Blockchain Services Infrastructure. Retrieved from: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/ebsi>.

- » Implementation of the European Directive on the Mandatory Exchange of Information on certain cross-border tax arrangements (“DAC6”).
- » Reporting income from the sharing and gig economy.
- » Implementation of a Digital Services Tax (“DST”).
- » Common Reporting Standard implemented for (certain type of) digital tokens and platforms/exchanges.
- » Combatting tax fraud and tax evasion by means of (more) robust tax systems enabled by blockchain technology.

It is fair to state that the aforementioned potential use cases may create a lot of additional research whereby a lot of questions will need to be addressed, including for example around privacy, the protection of taxpayer rights and the question whether the use of technology should be implemented as hard or soft law. A coordinated approach is required from the EU to actually make the implementation possible.

2. VAT and customs

When it comes to using blockchain technology to create more robust tax systems, by its nature, blockchain seems to be most suitable for transactional taxes. Not surprisingly, one of the most striking use cases often mentioned is to utilize blockchain to combat VAT fraud¹⁰⁵. Although the exact numbers are hard to assess, VAT fraud in the EU only is estimated to be EUR 50 billion problem annually¹⁰⁶. This amount is predominantly caused by phenomenon called carousel fraud or missing trader fraud. In short, carousel fraud happens when a series of connected businesses exploit cross-border VAT rules and disappear before the authorities catch on. Although some countries, such as Finland and Sweden¹⁰⁷, have already begun experimenting with how a blockchain-based system may combat VAT fraud, one of the more advanced initiatives seems to be developing within the private sector.

Despite the aforementioned interesting initiatives, the implementation of a blockchain-based EU system seems years away. The reason for this is not only the current state of the technology, but also the complexity of the problem that is to be solved. Typical obstacles for widespread adoption that are often heard include privacy concerns, the complexity of cross-border VAT rules and a lack of political consensus among member countries.

It almost goes without saying that blockchain technology also has great potential in the world of supply chains. This implies that there is also great opportunity for blockchain-based systems that would – for example – facilitate free trade. The technology may enable the exchange of

105 See, e.g., the Bloomberg Tax article “EU Inches Toward Blockchain in Fight Against VAT Fraud”, <https://news.bloombergtax.com/daily-tax-report-international/eu-inches-toward-blockchain-in-fight-against-vat-fraud-1> and G. Bulk, How blockchain could transform the world of indirect tax, https://www.ey.com/en_gl/trust/how-blockchain-could-transform-the-world-of-indirect-tax.

106 VAT Fraud, Economic Impact, Challenges and Policy Issues, Report from the European Parliament, PE 626.076 – October 2018.

107 Following from the aforementioned Bloomberg article, Finland is working on a proof-of-concept and Sweden is testing digitising receipts. Also, the United Arab Emirates are working on blockchain-based VAT system to combat fraud. See for example R. Ainsworth & M. Alwohaibi, BLOCKCHAIN, BITCOIN, AND VAT IN THE GCC: THE MISSING TRADER EXAMPLE, Law & Economics Working Paper NO. 17-05.

several trade documents (certificates of origin, bills of materials, bills of lading, shipping documents) so that typical trading barriers in these areas may be lifted and trade will become more efficient. Several initiatives are going on these topics, both inside and outside the EU and very few have currently risen beyond the proof-of-concept phase. It is expected that in this area a lot of initiatives will continue to emerge.

3. Other taxes

Another use case often heard in the world of taxation is around land registry rights, property, and real estate transfer taxes. The United Kingdom is one of the countries that is currently experimenting in this area¹⁰⁸. Notwithstanding the potential of the use case being explored, also for this type of solution it goes without saying that scalability is a potential impediment for (EU-wide) adoption.

In addition, several private initiatives around real estate investment platforms enabled by blockchain are currently ongoing (see *also* the example below on the potential tax implications surrounding such tax platforms).

Blockchain technology is also often referred to as to having great potential when it comes to transfer pricing, the rules determining intercompany pricing of transactions. Not only in supply chain may blockchain reliably facilitate the tracking and tracing of intercompany transactions, but smart contracts may also facilitate payments to safeguard at arm's length conditions when certain conditions are met. In the area of intangible assets, smart contracts may enable royalty payments by means of tokenizing the intellectual property and including business logic into smart contracts. This may be expanded to shared asset ownership, cost contribution arrangements, and treasury and lending transactions. In the (far) future, we can also envision that for certain types of comparable assets or services, specific tokens with certain pre-defined (basic) characteristics are being used to increase the comparability of assets and transactions, enabled by blockchain technology.

C. TAX TREATMENT – IDENTIFYING GENERAL STARTING POINTS

1. Classification of tokens as a precondition for taxation

The classification of tokens may hold income tax and VAT implications. Currently, there is no common EU framework for the classification of tokens. This means that individual assessments of token-characteristics must be conducted in order to assess if and to what extent tokens are subject to a tax regime in the country where the investor is a resident. Furthermore, differences between EU member states holds the potential of creating tax laws that are hybrid or inconsistent.

108 HM Land Registry (2019). Could blockchain be the future of the property market?. Retrieved from: <https://hmlandregistry.blog.gov.uk/2019/05/24/could-blockchain-be-the-future-of-the-property-market/>.

A key question, without a commonly-accepted answer in EU law¹⁰⁹, is how digital tokens are to be classified and how their distinct features should be accounted for¹¹⁰. As a basic guideline, based on their distinct features, tokens are distinguished between four categories: (i) security, *i.e.*, share-tokens representing a digital share (ii) asset/commodity, *i.e.*, a token representing ownership to gold, real estate, or art (iii) utility, *i.e.*, tokens representing benefits from participation in a network or platform such as (...) or (iv) currency/e-money, *i.e.*, tokens that can be used as a means of payment, like the examples of bitcoin or ether. Tokens may be placed in one or more of these categories creating the possibility of hybrid tokens which reflect that the token hold features in more than one category. In addition, comes that tokens can be bundled as other financial instruments leaving ample room for discussion on which features that are dominant in terms of taxation of underlying value.

Next to classifying tokens based on their distinct features comes the assessment of the usage of the digital tokens which most often is divided into the categories of payment tokens, investment tokens, and utility tokens¹¹¹. Occasionally, the usage of a token illuminates its core features which makes it easier to classify it. However, making individual intention behind holdings of tokens paramount to a domestic tax regime creates more individual assessments instead of standardization, which again may lead to regulatory arbitrage due to domestic differences in tax treatment of different tokens.

2. Taxable events

Generally, any event where tokens are used for payment or exchanged for goods or services is considered a taxable event. The same goes for buying, selling, trading, and transacting with tokens, including buying tokens, virtual assets, or cryptocurrency with other types of tokens, virtual assets, or cryptocurrency.

Furthermore, any conversion from digital token to fiat currency¹¹² is considered a taxable event. Profit or loss is determined based on the initial value when the digital token was purchased, and the transaction costs related to the conversion from fiat to digital token and digital token to fiat.

Mining operations may be seen as a taxable event. A distinction can be found between jurisdictions where mining is taxed based on an assessment of profit or loss calculated from the initial price of the token when mined and jurisdictions where mining may be taxed as a commercial activity subject to income tax with deductible expenses associated with it.

Holding digital tokens will trigger wealth taxation in most jurisdictions as long as the tokens are classified as an asset or investment. Utility tokens will, however, most often fall outside of such regimes. Hence, jurisdictional differences apply in terms of which tokens may form part of calculating wealth tax, in addition to the calculation of value of tokens that are not traded publicly or have a clear underlying value.

109 EC Consultation, p.7-8.

110 See ESMA Securities and Markets Stakeholder Group, Advice to ESMA, October 2018.

111 EC Consultation, p. 3.

112 Fiat is a reference to government issued currency that is not backed by a physical commodity, but rather by the government itself. Examples of Fiat money are USD; EUR, GBP etc. The term Fiat derives from the Latin Fiat ("let it be done") used in the sense of an order or resolution.

A particular question has been raised in terms of so-called “airdrops”. An airdrop is an event where holders of tokens receive new tokens due the initial ownership. Airdrops can also be effectuated in relation to an ICO where the investors are given a number of additional tokens, or as a hard fork where developers of a token create an additional branch of the original token using the same basic code¹¹³. Airdrops also include the event in which the receiver obtains a token issued by the producer for free by virtue of having a wallet that can accept the token, in order for the producer to establish a new ecosystem. The key feature of an airdrop is that tokens are allocated to holders of a pre-existing protocolled token, without the investor paying for them. Airdrops can be considered as ordinary income where the exchange between wallets can trigger a taxable event and thereby taxation on capital gains.

An important exemption from taxation is found in jurisdictions where internal transactions are not seen as taxable events. Such internal transactions are instances when an investor send tokens from one personal wallet to another, or from one personal exchange account to a different personal wallet. The decisive criterion is that the investor controls the private keys of both wallets or accounts. As an example of tax relief, some jurisdictions apply no tax or reduced tax for capital gains stemming from digital tokens as a result of staking. Staking refers to a situation where the investor locks up their tokens for long-term holding, where (s) he can earn more tokens through rewards or airdrops. Tax treatment of long-term holdings of tokens diverge between EU member states.

In the area of VAT, the ECJ ruling from 22 October 2015 is key¹¹⁴. In this ruling the Court of Justice of the European Union has ruled that the services of an exchange in exchanging bitcoin for a traditional currency is exempt from VAT on the basis of the “currency” exemption (Skatteverket v David Hedqvist Case C-264/14). Although this ruling pertained to the exchange of bitcoin to fiat currency, many EU countries have interpreted the ruling as applicable to all virtual currencies¹¹⁵. Following the ECJ decision the EU Value Added Tax Committee has issued guidance on the VAT treatment of digital tokens in several scenarios. Although this guidance is not binding, most EU countries follow this guidance. The guidance is depicted in the following table¹¹⁶:

113 To some extent it can be equated with the introduction of a new class of shares in a company without needing the consent of the shareholder assembly.

114 ECJ ruling 22 October 2015 Skatteverket v David Hedqvist Case C-264/14).

115 OECD (2020). Taxing Virtual Currencies: An Overview Of Tax Treatments And Emerging Tax Policy Issues. Retrieved from: www.oecd.org/tax/tax-policy/taxing-virtual-currencies-an-overview-of-tax-treatments-and-emerging-tax-policy-issues.htm, page 32.

116 *Ibid* p. 34.

Activity	Subject to VAT?	If so, exempt?
Use of bitcoin for acquiring goods or services	Out of scope: No VAT should be levied on the value on the bitcoin themselves	
Supplies of goods or services, subject to VAT, remunerated in bitcoin	Taxable: The supply of goods and services, subject to VAT and remunerated by way of bitcoin, would for VAT purposes be treated in the same way as any other supply. VAT should therefore be levied on the goods or services provided.	
Services supplied by digital wallets	Out of scope: A large majority of the services supplied by digital wallet providers are free of charge, which sees these transactions falling outside the scope of VAT.	
	Taxable: If, however, some digital wallet providers ask for payment of fees in exchange for their services, it seems that the transaction would be taxable.	Exempt: Such services could however be as exempt pursuant to Article 135(1)(e) of the VAT Directive, on the grounds of them being transactions directly concerning currency. Not exempt: It seems that services supplied by digital wallet providers could not be exempt pursuant to Article 135(1)(d) of the VAT Directive.
Mining activities	Out of scope: The fact that the payment of a transaction fee by a bitcoin user is not a necessary condition for successfully sending bitcoins (and thus for receiving a verification service supplied by the miner) may be indicative of there not being a direct link between the consideration and the service. Besides, the provision of a mining service does not create for the miner the right to receive a consideration in exchange, which could imply the non-existence of a legal synallagmatic relationship between him and the recipient of the verification services (the user whose transaction request the miner has validated).	
	Taxable: New bitcoin received automatically by the miner from the bitcoin system every time that a verification service is supplied could possibly be seen as constituting a consideration for a taxable service. Despite the fact the bitcoin transactions carried out for free are in theory possible, in practice bitcoin users pay fees (used as a default by most digital wallets); and it seems almost impossible to imagine users would be willing to wait days or weeks, before a transaction is verified (which could be the case if no fee is paid).	Exempt: Mining activities could be seen exempt pursuant to Article 135(1)(e) of the VAT Directive, on the grounds of them being directly concerning currency. Exempt: Mining activities could be treated exempt pursuant to Article 135(1)(d) of the VAT Directive on the basis of them fulfilling in the specific, essential, functions of an exempt supply (the transfer of bitcoin itself).
Services related to intermediation supplied by exchange platforms	Taxable: Services for consideration supplied by exchange platforms acting as intermediaries would be taxable.	Not exempt: Exchange services could not be seen as exempt pursuant to Article 135(1)(e) of the VAT Directive.

3. Remaining challenges

Due to the fast development of DeFi there are still a number of regulatory challenges when it comes to taxation. We will highlight three challenges that are core to any tax regime.

First, even though the token economy and DLT holds the promise of transparency, there may be circumstances where identification of beneficial owners of tokens are difficult. This may be due to the services of digital token service providers as custodians of *de facto* beneficial owners of tokens.

There are initiatives taken towards harmonizing the question on disclosure of beneficial owners, including regulating digital token service providers as facilitators. The role of digital token service providers as potential custodians adds to the concern of tokens, to some extent, resembling bearer shares which grants ownership to the individual that can prove holding of a token upon request. However, tokens can be co-owned or subjected to schemes where more than one investor must use their private keys in order to claim joint ownership. Without

harmonized legislation concerning beneficial ownership of digital tokens, there is a risk that ultimate beneficial owners will not be identified due to domestic differences in classifications.

Second, taxation requires a timing or taxable event. As discussed above, domestic differences can lead to legal hybrids where cross-jurisdictional token transactions and holdings are treated differently, resulting in a double non-taxation scheme.

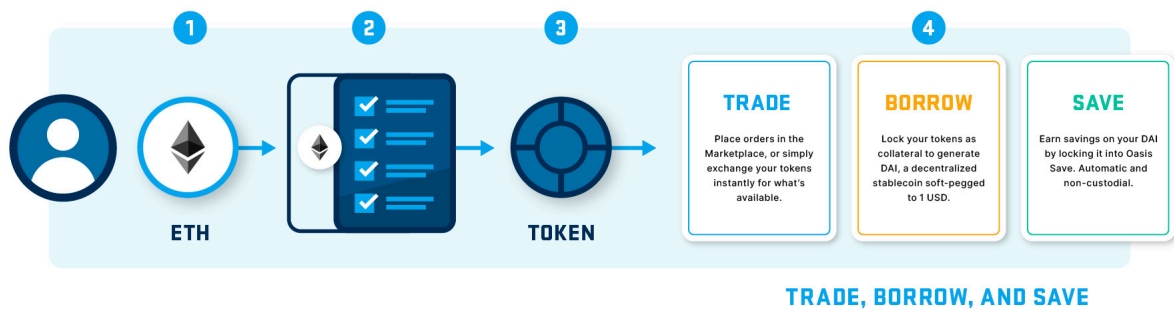
Third, finding the right value of tokens that are not “stablecoins” and backed by a fiat currency or commodities such as gold, nor traded publicly or in high volumes, is inherently difficult. To some extent, valuation of several tokens can be equated with valuation of tailor-made over-the-counter derivatives, where the exact value often is determined by the investor him/herself.

D. CASE STUDY – DECENTRALISED FINANCE

DeFi products are growing fast, and the complexity of the products are also following the growth together with tax-related questions. There are many different players within the DeFi landscape that are running non-custodial, permissionless smart contracts on the Ethereum blockchain and are considered to be decentralised.

With respect to lending, the smart contract works in the way that you provide cryptocurrency as collateral (step 1), then the collateral is locked up in the smart contract (step 2), which generates a new digital token (step 3) that is issued to the user as a loan. When the digital token is generated, users may start using the functionalities of the platform (step 4).

Typical categories of products offered on DeFi platforms can be *Trade*, where you can place orders or exchange your tokens. A second category is *Borrow*, where you can lock your tokens as a collateral to generate a new digital tokens used on the platform, and a third category is *Save*, where you can earn savings on your new digital token by locking it into a non-custodial smart contract on the DeFi platform.



The smart contract is non-custodial, which means that the user interacts with the DeFi protocol directly, and each user has complete and independent control of their collateral as long as it does not fall below a threshold for liquidation. If it falls below, the collateral will automatically be liquidated, and anyone at the platform may repay the debt in order to balance the situation. One can compare the process to a pawn broker, where you can deposit a watch or a ring, while here the collateral is a cryptocurrency.

The different trading, lending, and borrowing options of certain DeFi platforms raises several tax-related questions. However, we will focus on one of the main questions. Whether transferring cryptocurrency into a smart contract (step 1) and locking it up (step 2) are deemed as a taxable event in the form of a liquidation? – *i.e.*, a capital gain or loss should possibly be calculated and reported to the authorities.

As mentioned above, the main rule in most jurisdictions is that any event where tokens are used as a payment or exchange for goods or services is considered a taxable event. Hence, when you transfer a token from one wallet that you control, to another wallet that you do not control, it is considered to be a liquidation – *i.e.*, you have transferred the ownership rights, and a taxable capital gain or loss shall be calculated and reported to the tax authorities and eventually paid or deducted.

When executing step 1 and 2 in this example, the cryptocurrency has *de facto* been sent to another wallet/address – *i.e.*, to the smart contract. Hence, following the main rule this would be a taxable event. However, the question is: have you transferred the cryptocurrency to a wallet that you do not control – *i.e.*, who controls the smart contract?

To our understanding, the smart contract cannot be accessed by anyone else than the creator of it and the smart contract itself. Hence, it is partly controlled by the creator – *i.e.*, you may claim back your collateral in ETH if you repay the loan. It is also partly controlled by the smart contract itself, as it will execute automatically, without any possibility of stopping it, if you do not repay your loan or the value of your collateral drops below a certain threshold. Hence, one can say that it is the code that controls the smart contract. However, the smart contract is not a taxable subject that can or will report anything. The smart contract is rather an open-source code that the user has agreed to create her/himself.

To our knowledge, no court cases governing this question exist. Nor any known legislation or regulation. Hence, the parallel as mentioned above towards locking in cryptocurrency in a smart contract can be compared to going to a pawnbroker to deposit for example your watch in return for cash. The watch is still yours, as long as you repay the loan. However, if you do not pay, the pawnbroker can claim it. Hence, in our view, a transfer of a cryptocurrency into a smart contract is not to be considered as a liquidation in the form of triggering a taxable event such as calculating a capital gain or loss. As you *de facto* have not liquidated your locked up cryptocurrency. However, if the smart contract executes and liquidate your assets, we believe a capital gain or loss shall be calculated if local legislation requires so.

VI. Digital Tokens Outside The EU Financial Regime: Aml Considerations

A. INTRODUCTION

This section of the report focuses on the efforts of the EU to prevent money laundering and combat the financing of terrorism in the context of digital tokens. Specifically, it focuses on the 5th Anti-

Money Laundering Directive (“AMLD5”)¹¹⁷, which is a minimum harmonisation directive¹¹⁸ that brings digital tokens qualifying as virtual currencies (“VCs”)¹¹⁹, as per the definition in Subsection (B) (1) below, as well as VC service providers into the remit of EU anti-money laundering (AML) law. This report does not delve into the national laws of each of the now 27¹²⁰ EU member states but will mention EU member state law in passing where local law has gone beyond— “gold-plated”— AMLD5. While the focus of AMLD5 is aimed at preventing “anonymity” in the use of VCs, and in turn making them less susceptible to criminal use, increased regulation and co-operation will reduce the possibilities for regulatory arbitrage. However, it will not eliminate them altogether as Subsection B below discusses¹²¹. AMLD5 has also left a gap with respect to decentralised systems, where users can transact without intermediaries. In this respect, the FATF issued Recommendations which are more robust and will be discussed in Subsection C, since the EC and 14 out of 27 EU member states that also form part of FATF’s members will have to apply the revised Recommendations and FATF will conduct a second 12-month review in June 2021. It therefore merits a discussion on how the revised FATF Recommendations overlap with or diverge from AMLD5. Finally, as AMLD5 sets out to limit the risks presented by the cross border-nature of VC transactions, co-operation will be key. Statements by European bodies (as discussed in Section IV) indicate that the trend will be towards more harmonisation of anti-money laundering and combatting the financing of terrorism (“AML/CFT”) laws, co-ordination, and supervisory convergence.

B. AMLD5 – OVERVIEW

AMLD5 was published in the Official Journal of the EU on 19 June 2018¹²² and called upon EU member states to transpose it by 10 January 2020. As the name would imply, it is the fifth iteration of the AML directive that was first introduced by the EU in 1991. It is, however, the first to mention and regulate VC service providers. VC service providers operating in or out of the EU were largely unregulated from an AML perspective in the year and a half leading up to 10 January 2020, except for EU member states that adopted national legislation prior to this (examples include Malta and Estonia)¹²³. More specifically, VC service providers were—to use the words of AMLD5— “*under no Union obligation to identify suspicious activity*”¹²⁴.

AMLD6 came into force on 3 December 2020 and inter alia introduces a unified list of predicate offences, criminal liability for organisations, and increased international co-operation. While it does

117 5th Anti-Money Laundering Directive (2018/843/EU), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN>.

118 See footnote 17.

119 Virtual currencies is defined in AMLD5 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.

120 For purposes of this Paper, UK law will still be referred to, as the UK transposed legislation in line with AMLD5 before it left the EU on 31 January 2020. As of 28 April 2020, 6 countries have not notified the EC about whether AMLD5 has been transposed into their legislation, available at <https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX%3A32018L0843>.

121 See 19 April 2018 Statement by First Vice-President Timmermans, Vice-President Dombrovskis, and Commissioner Jourová on the adoption by the European Parliament of the 5th Anti-Money Laundering Directive: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_18_3429.

122 This coincided with the renewal of the EU four-year Policy Cycle, which was continued for the 2018 - 2021 period. The Policy Cycle was set up by the EU in 2010 to tackle the most significant threats to the EU posed by organized and serious international crime.

123 See, e.g., Chapter 590 of the Laws of Malta, “Virtual Financial Assets Act” (VFA Act). The VFA Act definition of an obliged entity, “subject person” includes issuers of virtual financial assets and those offering virtual financial asset services. In 2017, Estonia was also one of the first EU member states to implement AMLD5 by bringing digital token exchanges and storage activities into the remit of AML/CFT regulations. Section 3 (9) of the Anti-Money Laundering Act and Terrorism Finance Act in Riigi Teataja (2017) Money Laundering and Terrorism Financing Prevention Act. Available at: <https://www.riigiteataja.ee/en/eli/517112017003/consolide>.

124 Recital 8, AMLD5.

not explicitly make any changes to the AML/CFT regulation of VCs, it does make some changes in the field of cooperation—see Section (B)(5)(D) below.

1. Definition of VC

The starting point for every regulatory regime should include a common understanding of the definition of what it seeks to regulate—AML5 defines VCs as:

- » A digital representation of value that is not issued or guaranteed by a central bank or a public authority (e.g., proposed Swedish e-Krona¹²⁵ would not be a VC within the meaning of AML5);
- » Not necessarily attached to a legally established currency (VCs can be pegged to external references such as fiat currencies, commodities with a fixed exchange rate system, underlying assets, or even other VCs, *i.e.*, “stablecoins”);
- » Does not possess a legal status of currency or money (e.g., ‘e-money’);
- » Accepted by natural or legal persons as a means of exchange and which can be transferred, stored, and traded electronically.

The latter point requires some further clarification. To be classified as a VC, the token must be accepted as a means of exchange, have the technical capability of being “transferred” (from one blockchain user to another), “stored” (e.g., in a wallet), and “traded electronically” (on VC exchanges and in VC markets)—this would exclude tokens with a “lockup” mechanism, which restricts their transfer. While Recital 10 of AML5 states that VCs “*could also be used for other purposes and find broader applications such as means of exchange, investment, store-of-value products or use in online casinos*” the definition in of VC in the AML5 does not provide for this. In this respect, it is narrower than the FATF definition of virtual assets (“VAs”)¹²⁶ which covers investment tokens, utility tokens, and perhaps, in certain use cases, in-game tokens—all capable of being used for money laundering.

2. Who or what does AML5 regulate?

AML5 states that “[t]he anonymity of virtual currencies allows their potential misuse for criminal purposes”. AML5 regulates and increases oversight of two kinds of service providers:

- » “[P]roviders engaged in exchange services between virtual currencies and fiat currencies” (“VC exchanges”).
- » Custodian wallet providers, which means “an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies”.

¹²⁵ See <https://www.riksbank.se/en-gb/payments--cash/e-krona/>.

¹²⁶ Interestingly, Consideration 8 of the European Commission proposed MiCA states that “Any definition of ‘crypto-assets’ should therefore correspond to the definition of ‘virtual assets’ set out in the recommendations of the Financial Action Task Force (FATF)”.

Just like the other ‘obliged entities’¹²⁷ listed in AMLD5 and AMLD 4¹²⁸, the AML duties fall on the person providing the VC service. More specifically, these providers are the “gatekeepers” of the points where fiat currencies are commonly converted into VCs or where VCs are converted into fiat currencies (e.g., VC exchanges). According to AMLD5, obliged entities must conduct know your customer (“KYC”) / customer due diligence checks (“CDD”)¹²⁹ prior to commencing and during the course of business relationships, keep records of customer dealings, conduct risk assessments, understand the purpose of the business relationship, identify beneficial owners, monitor transactions, and submit suspicious activity reports¹³⁰ to competent authorities. Custodial wallet providers and VC exchanges must also be registered with each EU member state’s competent authorities, such as Germany’s BaFin¹³¹ or the French AMF¹³².

Part of the rationale for regulating VCs from an AML perspective is to counteract the anonymity associated with the use of VC and so that “*competent authorities should be able, through obliged entities, to monitor the use of virtual currencies*”¹³³. AMLD5 therefore seeks to enable Financial Intelligence Units (FIUs) “*to obtain information allowing them to associate virtual currency addresses to the identity of the owner of virtual currency*”¹³⁴. Trying to regulate elements of the blockchain ecosystem (e.g., a mining pool or nodes)¹³⁵ may be challenging, even though the EU Parliament has explored in a report published in April 2020 (“EU Parliament Report”) the idea of regulating miners¹³⁶. AMLD5 has instead chosen to focus on certain VC “intermediaries” – in-keeping with traditional financial crime and AML laws that focus on intermediaries. Exchanges and wallets, as the now *de jure* (but perhaps not *de facto*) intermediaries of the VC economy, can identify the users behind VC transactions. In fact, since (or perhaps in response to) AMLD5’s 10 January 2020 implementation deadline, several VC companies have either relocated or are winding up¹³⁷.

3. VC Exchanges

The following overview of how fiat currency enters and exists the VC system through exchanges also illustrates both the benefits and the shortcomings of AMLD5.

- » Under AMLD5, a VC exchange is an ‘obliged entity’ and will be required to perform extensive KYC and CDD procedures when establishing a business relationship¹³⁸. In practice this would

127 See Article 2(1) of AMLD 4.

128 4th Anti-Money Laundering Directive (2015/849/EU).

129 As AMLD5 is a minimum harmonisation directive, it is up to EU member states to determine whether all transactions—whether occasional or part of an ongoing business relationship—will need to be subject to CDD. This could include identifying the customer and verifying their identity and the veracity of the information provided. See Articles 11 and 13 of AMLD 4.

130 Suspicious Activity Reports (SARs) or Suspicious Transaction Reports (STRs): if suspicious activity is identified and there are reasonable grounds to suspect funds come from the proceeds of crime then the entity needs to make a SAR or STR to the FIU.

131 BaFin (2017). Virtual currency. Retrieved from: https://www.bafin.de/EN/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node_en.html.

132 Article 1(29) of AMLD5 amending Article 47(1) AMLD 4.

133 Recital 8, AMLD5.

134 Recital 9, AMLD5.

135 <https://coinrivet.com/es/enemy-mine-crypto-mining-pools-linked-to-crime-and-terrorism/>.

136 European Parliament (2020). Crypto-assets: Key developments, regulatory concerns, and responses. Retrieved from: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU\(2020\)648779_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf), pp. 53-54.

137 Deribit and Kyberswap have relocated. Cryptocurrency payments firm BottlePay, cryptocurrency mining pool Simplecoin, and bitcoin gaming platform Chopcoin are among some of those firms who have closed down.

138 Article 11 of AMLD 4 states that EU member states shall ensure that obliged entities apply customer due diligence measures in the following circumstances [selected examples]:
(a) when establishing a business relationship;

mean collecting and verifying a customer's means of identification (both private individuals and corporate entities)— including government-issued identity cards or passports, phone numbers, physical address, email address, and/or a utility bill. A customer may also be asked to declare their VC addresses, source of funds and wealth, account numbers, IP address, or location information, which would facilitate the linking of VC wallet addresses to the beneficial owners and in turn clamping down on the use of anonymous addresses on VC exchanges. Ongoing CDD may also be warranted¹³⁹.

- » Once a person has successfully opened an account, they can use fiat or VC to buy other VCs. Reading AMLD5 at face value would suggest that a VC-only exchange, which provides the means for exchanging one VC for another, would not be subject to AMLD5 as its customers will buy and sell VC—not fiat. These VC exchanges usually require that their customers fund their accounts by depositing VC into the pooled exchange wallet. The exchange will therefore be acting as a custodial wallet—an obliged entity—by safeguarding customers' private keys in its wallet¹⁴⁰. Without appropriate measures in place, money launderers could abuse this stage and use it as the “placement” stage of money laundering¹⁴¹—where illicit proceeds enter the financial system. However, it is possible that VC-only exchanges could be used at the “layering stage”, which is described in the following paragraph. Here, AMLD5 and the industry are trying to stop “*terrorist groups [that] may be able to transfer money into the Union financial system or within virtual currency networks by concealing transfers or by benefiting from a certain degree of anonymity on those platforms*”¹⁴².
- » By the time VC is purchased on a fiat-to-crypto exchange, there is a trace and money launderers would seek for ways to hide their trail. The VC's audit trail can be obfuscated through mixing/tumbling anonymity-enhancing services or CoinJoin¹⁴³. AMLD5 does not include providers of tumbler or mixer services as obliged entities¹⁴⁴. Once the VC wallet address is tumbled, a money launderer could then exchange the VC bought on exchange 1 for a privacy VC or VC with privacy features (e.g., Zcash (ZEC), Monero (XMR), Dash (DASH),

(b) when carrying out an occasional transaction that:

(i) amounts to EUR 15 000 or more, whether that transaction is carried out in a single operation or in several operations which appear to be linked; or

(ii) constitutes a transfer of funds, as defined in point (9) of Article 3 of Regulation (EU) 2015/847 of the European Parliament and of the Council (1), exceeding EUR 1 000;

(e) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption, or threshold;

(f) when there are doubts about the veracity or adequacy of previously obtained customer identification data.

139 Article 1(9)(b) of AMLD5, updating Article 14(5) of AMLD 4.

140 Exchanges do not always have their own wallet and sometimes hold private keys in addition to the wallet services provider. This is the case with multi-signature wallets. See, for example, BitGo's terms and conditions, which states that BitGo controls only one of the three private keys for a “Digital Asset” wallet provided by the service: <https://www.bitgo.com/terms>.

141 FAFT. Virtual Assets. Retrieved from: [https://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets.html?hf=10&b=0&s=desc\(fatf_releasedate\)](https://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets.html?hf=10&b=0&s=desc(fatf_releasedate)).

142 Recital 8, AMLD5.

143 The Wasabi Wallet uses CoinJoin, which is a non-custodial, privacy-focused Bitcoin *wallet* that implements trustless *coin* shuffling. For more information on CoinJoin, See <https://www.investopedia.com/terms/c/coinjoin.asp>.

144 According to Europol, more than forty percent of online transactions used Bitcoin, virtual currency mixers, and tumblers for illegal ends. See European Monitoring Centre for Drugs and Drug Addiction and Europol (2017), *Drugs and the darknet: Perspectives for enforcement, research, and policy*, EMCDDA–Europol Joint publications, Publications, Office of the European Union, Luxembourg.

Beam (BEAM)¹⁴⁵¹⁴⁶ on exchange 2. Given that, according to the EU Parliament Report, illegal users tend to prefer mixers and tumblers, it is likely that such privacy-enhancing coins would be used as an added—not the main—layer of concealment¹⁴⁷. A person could also make off-chain transactions or exchange their tumbled VC on exchanges based in jurisdictions without AML laws. Comparing this process to traditional money laundering, this would be the “layering stage”—to separate the illicit money from its source.

- » Finally, the VC-denominated illicit proceeds would then “exit” the system for “integration”¹⁴⁸ into the legitimate economy through means such as: (a) exchanges, which would leave a trail; (b) by transferring the VC onto a hardware wallet, which is not regulated by AMLD5, and giving the hardware wallet to someone in exchange for money; (c) through VC ATMs¹⁴⁹, if the ATM does not require any KYC; or (d) by making purchases with anonymity-enhanced VCs.

4. VC Custodian Wallet Providers

Wallet addresses (similar to an IBAN in bank transfers) and VC transaction IDs (e.g., dates, values, and counterparties) are publicly visible on a blockchain but the owners of the VCs are not. This is what AMLD5 sets out to prevent. At any given moment, a VC is attached to a wallet address on the blockchain, which has a private key. Private keys are long hexadecimal codes known only to the wallet holder and must match with a public key in order to make a VC transfer¹⁵⁰. A VC transfer is like a message broadcasted to the network that is signed by the private key, which must match the public address of the wallet the VC will be assigned to. A node will pick this message and verify the transaction by matching the public key with the private key, passing it on to other nodes until the whole network “knows” it and either accepts the validity of the transaction or rejects it. If the public and private keys do match, the balance in a wallet will increase or decrease accordingly. This illustrates the importance of bringing wallet providers within the scope of AMLD5, as wallet addresses are “pseudonymous” — as they do not, in themselves, reveal the identity of the owner —and CDD helps in linking the real-

145 Beam is based on the confidential transaction protocol MimbleWimble and has a transaction auditability feature: <https://beam.mw/faq/what-is-auditability>.

146 EU officials have discussed the following cryptocurrencies, making a distinction between optional anonymous coins (e.g., Dash), pseudonymous coins (e.g., NEO's Gas, IOTA, Ada, bitcoin and Lumens) and anonymous coins (e.g., Monero): Monero is anonymous due to its use of ring confidential transactions and stealth addresses that ensure there are no links on the blockchain between the sender's and the recipient's address, as well as its ease of convertibility to any major virtual token. It describes Dash as having a privacy option through the presence of PrivateSend, which obscures the origins of a user's funds through mixing. Interestingly, it does not mention Zcash. However, privacy coin developers maintain that their protocols can comply with FATF recommendations and the Travel Rule since a VASP has done KYC on its customer and can therefore share information of its transactions with other VASPs.

147 EU Parliament Report, p. 28.

148 The Italian National Council of Notaries has advised notaries to make STRs for every real estate purchase with virtual currencies. See Quesito Antiriciclaggio n. 3-2018/B, Consiglio Nazionale del Notariato (13 March, 2018), http://www.dirittobancario.it/sites/default/files/allegati/quesito_antiriciclaggio_n._3-2018-b.pdf.

149 See p. 51 of the 2018 study commissioned by the European Parliament, entitled “Virtual currencies and terrorist financing: assessing the risks and evaluating responses”, [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU\(2018\)604970_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf). For example, Dutch law has differentiated between providers of physical ATMs that offer such exchange services but does not include shop owners who only make such ATMs available. See the Explanatory Memorandum to the Act Implementing Amendments to the Fourth Anti-Money Laundering Directive (AMLD5 Implementation Act), <https://www.rijksoverheid.nl/documenten/kamerstukken/2019/07/02/memorie-van-toelichting-implementatiewet-wijziging-vierde-anti-witwasrichtlijn>. In Germany, these ATMs are considered as companies conducting “cross-border proprietary trading” since VCs are considered as ‘financial instruments’: https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Verbrauchermitteilung/unerlaubte/2020/meldung_200304_KKT_UG_Berlin_en.html.

150 See the following for an explanation: <https://medium.com/coinmonks/blockchain-public-private-key-cryptography-in-a-nutshell-b7776e475e7c>.

world identity behind the wallet with the wallet address itself. AMLD5 therefore requires VC custodian wallet providers to comply with its regulatory framework.

Wallets can be both “hot” (online/connected to the internet) and “cold” (offline) wallets. For VC custodian wallet providers, the crucial element is custodianship. A VC wallet provider wondering whether there is a duty to comply with AMLD5 would begin by asking whether they “safeguard” private cryptographic keys. While most providers of VC wallets offer their customers wallets in which their private key is stored¹⁵¹, VC wallet providers could be “non-custodian”—and therefore fall outside the scope of AMLD5—if they do not control or have access to the private keys and merely provide users with the means to store their private keys themselves. In short, the responsibility of safeguarding private keys is the owner’s own responsibility. This raises further issues when one considers that a person can hand over their VC hardware wallet, e.g., a USB stick or software that runs on a user’s hardware, at which point the person physically receiving the hardware wallet becomes the new “owner”. EU member states are of course free to further elaborate on the definition of a “custodian”¹⁵² or perhaps prescribe minimum standards for cybersecurity to be complied with when offering custodial wallet services for VCs¹⁵³.

5. Gaps left by AMLD5

VC exchanges and custodian wallet providers are intermediaries that facilitate the inter-connections between the VC and fiat markets. However, these obliged entities only represent a part of the VC ecosystem. Interestingly, AMLD5 acknowledges that *“a certain degree of a large part of the virtual currency environment will remain anonymous because users can also transact without such providers [VC exchanges and custodian wallet providers]”*. The EC has also identified gaps during its 24 July 2019 supranational risk assessment¹⁵⁴, which are custodial wallet providers that do not safeguard keys on behalf of their customers; exchanges from VCs or VAs to other VCs or VAs; and *“participation in and provision of financial services related to an issuer’s offer and/or sale of a virtual asset”*. In the EBA 5 February 2020 Consultation Paper on revised guidelines on AML/CFT risk factors¹⁵⁵ and in the EBA’s 1 March 2021 ML/TF Risk Factors Guidelines¹⁵⁶, the EBA states that the following three out of four points should also be considered as VC businesses, which points to the shortcomings of AMLD5:

-
- 151 Additionally, custodial wallet providers are beginning to enhance the appeal of their services through, for example, insurance. They are also developing methods to allow VC owners to stake their assets or exercise governance rights while in custody. See <https://www.edisongroup.com/wp-content/uploads/2020/02/Diginexreport270220.pdf>.
- 152 The German Act Implementing the Amending Directive on the Fourth EU Anti-Money Laundering Directive (Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie) (Federal Law Gazette I of 19 December 2019, p.2602) incorporates “crypto custody business” into the German Banking Act (Kreditwesengesetz - KWG). Germany goes beyond AMLD5 in Section 1 (1a) sentence 2 no. 6 of the KWG, which defines crypto custody business as providing custody, management, and backup services for crypto-assets or for private cryptographic keys which are used to keep, store, or transfer crypto-assets for others. This is an activity that must be licensed.
- 153 EU Parliament Report, pp. 62-64.
- 154 See EC, “Commission Staff Working Document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities”, SWD(2019) 650 final, July 2019, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019SC0650&from=EN>, p. 103.
- 155 Draft Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (“The Risk Factors Guidelines”), amending Guidelines JC/2017/37 https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Consultations/2020/Draft%20Guidelines%20under%20Articles%2017%20and%2018%284%29%20of%20Directive%2028EU%29%202015%20on%20customer/JC%202019%2087%20CP%20on%20draft%20GL%20on%20MLTF%20risk%20factors.pdf.
- 156 Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions under Articles 17 and 18(4) of Directive (EU) 2015/849 (EBA/GL/2021/02).

1. *“Operating as a VC trading platform that effects exchanges between virtual currencies” – crypto-to-crypto exchanges*

AMLD5 does not expressly bring crypto-to-crypto exchanges—providers that are engaged in exchanging one VC for another—within its scope. However, as these exchanges usually require that their customers fund their accounts by depositing VC into the exchange wallet, the exchange will also be an “obliged entity” if it holds private keys and therefore acts as a custodian wallet provider. Exchanges do not always have their own wallet and sometimes hold private keys together with the wallet services provider. This is the case with multi-signature wallets¹⁵⁷.

2. *“Arranging, advising or benefiting from ‘initial coin offerings’ (ICOs)”*

Those who issue and sell VCs are at first glance not listed as obliged entities under AMLD5. ICOs that are not listed on exchanges and conduct little to no KYC on buyers may allow criminals to swap VC that originated from illicit activity or “tumbled” VCs for freshly-minted tokens that can then be sold for fiat currency¹⁵⁸. Mining coins is also another way that criminals, through agents, can gain a hold of coins without a “tainted” history. The benefit of “clean” and freshly minted coins is that they will not be flagged by the transaction monitoring services mentioned in Subsection D below.

The EU Parliament Report states that another challenge relates to financial service providers active in the *“participation in and provision of financial services related to an issuer’s offer and/or sale of a crypto-asset”*. Regulating financial or professional service providers who are instrumental in assisting with ICOs could be a solution for the above and, indeed, some EU Member States have already done so¹⁵⁹.

3. *“Operating as a VC trading platform that allows peer-to-peer transactions” - decentralised exchanges and atomic swaps*

It is said that 90% of VC economic activity occurs on centralised custodial exchanges¹⁶⁰ and may explain why decentralised exchanges are outside the remit of AMLD5. Royal United Services Institute, a leading defence and security think-tank in the UK, noted in a report¹⁶¹ the challenges of decentralised systems:

Some P2P exchanges are akin to a forum where buyers and sellers come together, with the added benefit of an escrow facility to prevent scams. Other exchanges operate on the basis of (self-executable) smart contracts and are often known as decentralised

157 See, for example, BitGo’s terms and conditions, which states that BitGo controls only one of the three private keys for a “Digital Asset” wallet provided by the service: <https://www.bitgo.com/terms>.

158 This reflects the results of ESMA Report, p. 36. The same could be true for airdrops. Airdrops are a distribution of tokens, which is usually for free, to individuals in order to attract more users or generate publicity. Recipients are not necessarily required to provide KYC upon receiving such tokens, although most airdrops also require a person to have an “active” address in order to receive coins.

159 For example, VFA agents in Malta who are responsible for confirming that the ICO white paper is in compliance with the requirements of Maltese law on this topic, as defined in Article 7 of Chapter 590 of the Laws of Malta (the VFA Act) and the Financial Instrument Test and submitting the white paper to the Malta Financial Services Authority. The VFA Agent must also perform due diligence on the issuers of the ICO.

160 6 March 2020 speech by Therese Chambers (Director of Retail and Regulatory Investigations, FCA, “Unstable coins: crypto-assets, financial regulation and preventing financial crime in the emerging market for digital tokens”).

161 See p. 16 of From Intention to Action: Next Steps in Preventing Criminal Abuse of Cryptocurrency, Anton Moiseienko and Kayla Izenman. Occasional Papers, 10 September 2019.

exchanges. In its most ambitious manifestation, a P2P exchange can be maintained by a dispersed community of users and therefore be highly resistant to attempts at regulating or closing it down. This can be potentially achieved through the use of a decentralised application (“DApp”), a software programme based on smart contracts.

A decentralised exchange (DEX) is a VC exchange that allows for peer-to-peer trading and which operates without a supervisor and without a central wallet, thereby allowing users to retain ownership of their private cryptographic keys. Atomic swaps¹⁶² are also a form of peer-to-peer transfers across different blockchains that allows users to exchange VC without them ever being transferred to an intermediary. Decentralised systems therefore present a higher AML/CFT risk because there is no intermediary *per se* to regulate and therefore potentially weakens the role of centralised VC service providers¹⁶³. This equally applies to DeFi, which runs through decentralised exchanges. DEX and DeFi are therefore not likely to be subject to AMLD5 nor likely to be classified as a Virtual Asset Service Provider¹⁶⁴.

4. *Those who provide, or are involved in, the technology*

While this fourth point was not suggested in the EBA Report, it was discussed in the EU Parliament Report. It states that other AMLD5 challenges include miners and coin inventors. Discussion is also increasing around user registration for all activities¹⁶⁵ and coin blacklisting¹⁶⁶. However, with respect to coin inventors, it is arguable that to put the onus of AML duties on those who merely provide technological tools would also re-shape EU AML/CFT law as we know it. Further, it would go against AMLD5 Recital 8, which suggests “*a balanced and proportional approach, safeguarding technical advances and the high degree of transparency attained in the field of alternative finance and social entrepreneurship*”.

C. FATF

The FATF is an inter-governmental body that sets international standards that aim to combat money laundering, terrorist financing and other related threats to the integrity of the international financial system. It comprises 37 member jurisdictions and two regional organisations. FATF issues recommendations and member countries are expected to enforce them or will otherwise be held to account. FATF’s tools such as mutual evaluations, naming and shaming “*high-risk jurisdictions subject to a call for action*” (“blacklist”), or placing countries under increased monitoring (“grey list”) have proven to be effective in encouraging enforcement by non-member countries.

On 21 June 2019, FATF adopted the Guidance for a *Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (“2019 Guidance”)¹⁶⁷ and an Interpretive Note to Recommendation 15 on New

162 See pp. 38-39, 77 of TAX3 Study on cryptocurrencies and blockchain: <https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf>.

163 EU Parliament Report, pp. 54-55.

164 See <https://theconversation.com/decentralised-finance-calls-into-question-whether-the-crypto-industry-can-ever-be-regulated-151222>.

165 EU Parliament Report, p. 58.

166 *Ibid.*, pp. 64-65.

167 FATF (2019). Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Retrieved from: <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html>.

Technologies (INR 15)¹⁶⁸. INR 15 describes binding measures applicable to countries and VA service providers (“VASP”), as well as other obliged entities that engage in or provide VA products and services. FATF members had until June 2020 to adopt the recommendations, at which time FATF released a 12-month review report¹⁶⁹. FATF also released a report on 14 September 2020 entitled “Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing”¹⁷⁰.

Although the EC and 14 EU member states are members of FATF, AMLD5 is not as stringent as the FATF 2019 Guidance and INR 15. While VASPs are broader than AMLD5’s list of obliged entities (VASPs include crypto-to-crypto exchanges; transfer of VAs; safekeeping of VAs; and activities related to issuing or underwriting VAs), the biggest divergence from AMLD5 is INR 15 paragraph 7(b) R16, which states that “[c]ountries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information” and that all other requirements set forth in Recommendation 16 apply to VASPs. Previously, Recommendation 16—the “travel rule”—did not apply to VASPs and only imposed the requirement on financial institutions to collect and transmit information about the originator and the beneficiary of a wire transfer transaction to other financial institutions. The 2019 Guidance¹⁷¹ describes how this applies to VASPs:

VASPs or other obliged entities that engage in VA transfers, including the obligations to obtain, hold, and transmit required originator and beneficiary information in order to identify and report suspicious transactions, monitor the availability of information, take freezing actions, and prohibit transactions with designated persons and entities.

[...]

The required information includes the: (i) originator’s name (*i.e.*, the sending customer); (ii) originator’s account number where such an account is used to process the transaction (*e.g.*, the VA wallet); (iii) originator’s physical (geographical) address, or national identity number, or customer identification number (*i.e.*, not a transaction number) that uniquely identifies the originator to the ordering institution, or date and place of birth; (iv) beneficiary’s name; and (v) beneficiary account number where such an account is used to process the transaction (*e.g.*, the VA wallet). It is not necessary for the information to be attached directly to the VA transfer itself.

The above “travel rule” therefore requires VASPs to gather data on both the recipient and the sender, as well as liaising with other VASPs. Conversely, the AMLD5 merely requires recordkeeping and the submission of data to FIUs upon request.

While VASPs are therefore subjected to the AML/CFT obligations to which the traditional financial service providers are, systems which can assist in complying with the respective duties are only beginning to develop¹⁷². In fact, on 21 August 2020, it was announced that three Swiss crypto

168 In October 2018, the FATF made changes to its Recommendations to extend its scope to financial activities involving virtual assets and added “virtual asset” (VA) and VASPs to its glossary.

169 FATF (2020), 12-month Review Virtual Assets and VASPs, FATF, Paris, France, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPs.pdf>

170 FATF (2020), Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets, FATF, Paris, France, www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html.

171 2019 Guidance, paragraph 114.

172 For example, CipherTrace’s Travel Rule Information Sharing Architecture (TRISA) makes it easier for companies to comply with the FATF travel rule as it applies public key infrastructure to identify and verify VASPs. See the white paper here: <https://ciphertrace.com/wp-content/uploads/2019/08/TRISA-Enabling-FATF-Travel-Rule-V4.pdf>.

companies completed the first automated Bitcoin transaction using the FATF Travel Rule Protocol¹⁷³. When executing payment transactions, the traditional institutions have recourse to the SWIFT system. The blockchain transactions are currently restricted in technical terms, since most blockchain systems operate only pseudonymous transactions – the originator and the beneficiary are identified via crypto addresses and the persons behind such addresses remain unknown. Therefore, at present, it is technically difficult to pass on data on the originator and the beneficiary (which is also why FATF allows for the transmission of information to take place independently of the initial blockchain transaction). In Switzerland, FINMA's interpretation goes beyond what is required by the 2019 Guidance. For example, Swiss VASPs now limit their transactions to external wallets that belong to their own clients and prove the ownership over the wallet through “*proof of wallet ownership signature*”, i.e., manually¹⁷⁴. FINMA believes that exemptions would create an imbalance between unregulated and regulated service providers and would ultimately defeat the purpose of the law. A similar pattern can be observed with EU member states that have gold-plated AMLD5¹⁷⁵.

D. ENFORCEMENT AND COORDINATION

In addition to AMLD5, there is also a growing amount of non-legally binding guidance in the EU that relates to AML and VCs¹⁷⁶. The EU is moving closer towards increased harmonisation and co-operation for money laundering enforcement. This is seen in AMLD6 (which *inter alia* introduces a unified list of predicate offences, criminal liability for organisations, and increased international co-operation. It also introduces cybercrime as a predicate offense. The addition of cybercrime as a predicate offense is welcome, as the value of VC funds gained from online fraud, phishing, ransomware and hacks has significantly increased. AMLD6 also extends legal liability— e.g. money laundering offences involving VC—to legal persons), the calls for creating a coordination and support mechanism that encourages and facilitates the cross-border work of FIUs¹⁷⁷, conferring certain responsibilities and powers for AML supervision to an EU watchdog¹⁷⁸, the establishment of the European Public Prosecutor's Office and by granting a stronger role to the EBA¹⁷⁹. There is also a plan for a revised AML/CFT landscape in the EU, which is discussed in the 7 May 2020 Communication from the European Commission (EC) on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing (C(2020) 2800 final).¹⁸⁰

173 <https://www.coindesk.com/crypto-companies-fatf-bitcoin-transaction>.

174 For further information please consult: <https://www.newrealityblog.com/2020/02/17/the-fatf-travel-rule-for-vasps-that-travelled-to-switzerland-with-greater-strictness/>.

175 Examples include the UK and Austria. In the UK, AMLD5 was transposed into domestic law via the Money Laundering and Terrorist Financing (Amendment) Regulations 2019 and extended the scope of persons subject to AML laws to include: VC Exchange Platforms and Custodian Wallet Providers who must comply with the UK's AML regime. Section 14A states that VC Exchange Platform activity covers (a) exchanging or arranging or making arrangements with a view to the exchange of crypto-assets for money or money for crypto-assets, (b) exchanging, or arranging or making arrangements with a view to the exchange of, one crypto-asset for another, or (c) operating a machine which utilises automated processes to exchange crypto-assets for money or money for crypto-assets. In Austria, companies offering VC services are now subject to the supervision and control of the Financial Market Authority (FMA) as per the Financial Market Money Laundering Act (Finanzmarkt-Geldwäschegesetz or FM-GwG). The new regulations will affect activities related to wallet providers, crypto exchanges, peer-to-peer service providers, issuers of digital tokens and digital token operators.

176 Such as the guidance published by ESMA, the EBA and European Insurance and Occupational Pensions Authority (EIOPA) e.g., 16 December 2019 Final Report on Joint guidelines on cooperation and information exchange for the purpose of Directive (EU) 2015/849 between competent authorities supervising credit and financial institutions, https://www.esma.europa.eu/sites/default/files/library/joint_guidelines_on_cooperation_and_information_exchange_on_aml_-_cft.pdf.

177 See (47). Para. 17 of the 5 December 2019 Council conclusions on strategic priorities on AML/CFT, as adopted by the Council (ECOFIN).

178 *Ibid*, para. 20. See also the EU Parliament Report, pp. 58 – 59.

179 Article 85 TFEU and Regulation (EU) 2018/1727.

180 See the 19 August 2020 response by the EBA to the European Commission's Public Consultation on an AML/CFT Action Plan and the Establishment of an EU Level AML/CFT Supervisor, https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Other%20publications/2020/923773/EBA%20response%20to%20the%20consultation%20on%20the%20Commission%27s%20AML%20action%20plan%20final%20for%20publication.pdf; the 10 September 2020 Opinion of the European

EBA

Regulation (EU) 2019/2175 made the EBA the sole competent authority to carry out the tasks to “lead, coordinate and monitor” the AML/CFT efforts of all EU financial services providers and competent authorities¹⁸¹. With regard to the “monitor” aspect, the EBA intends to monitor the implementation of EU AML/CFT standards by competent authorities and financial institutions. The primary tool will be AML/CFT focused peer reviews and the EBA’s new power to ask competent authorities to take action if there are indications or evidence that financial institutions have breached EU law. As a last resort, it can exercise the power to investigate¹⁸².

EPPO

Article 86 of the Treaty on the Functioning of the European Union (“TFEU”) introduced the Public Prosecutor’s Office to combat crimes affecting the financial interests of the EU. The European Public Prosecutor’s Office (“EPPO”) is scheduled to become operational at the end of 2020 and, once this happens, will act as the EU’s independent and decentralised prosecution office, with the competence to investigate, prosecute and bring to judgment crimes against the EU budget, such as fraud, corruption, or money laundering as defined in AMLD 4¹⁸³.

Europol

The EU Agency for Law Enforcement Cooperation (“Europol”) is, as the name implies, the EU’s law enforcement agency. Europol supports the 27 EU member states in the fight against serious organised crime and terrorism, including cybercrime, international drug trafficking, money laundering, fraud, the counterfeit of euros, and the trafficking in human beings.

Recent Europol enforcement operations have included:

- » A Europol-led police operation that led to the arrest of three people who allegedly ran the Wall Street Market, supposedly the world’s second-largest “dark web” marketplace. In the process, authorities also seized the site’s servers, more than EUR 550,000 in cash, bitcoin and Monero¹⁸⁴.

Banking Authority on the future AML/CFT framework in the EU (EBA/OP/2020/14), https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2020/931092/Opinion%20on%20the%20future%20AML%20CFT%20framework%20in%20the%20EU.pdf; and the EBA Report On The Future AML/CFT Framework in the EU Response to the European Commission’s Call For Advice on Defining the Scope of Application and the Enacting Terms of a Regulation To Be Adopted in the Field of Preventing Money Laundering and Terrorist Financing (EBA/REP/2020/25), https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2020/931093/EBA%20Report%20on%20the%20future%20of%20AML%20CFT%20framework%20in%20the%20EU.pdf. EBA/OP/2020/14 and EBA/REP/2020/25 recommend that the European Commission has regard to recent revisions to the FATF standards and guidance regarding ‘virtual assets’ and ‘VASPs’, and changes to the scope of EU AML/CFT legislation to bring activities that are not currently covered, such as crypto-to-crypto exchanges within the scope of the AMLD in line with the FATF’s Recommendations and the FATF’s evolving approach.

181 In 2019, the European legislature consolidated the AML/CFT mandates of the EBA, EIOPA and ESMA within the EBA. It also gave the EBA a legal duty to contribute to preventing the use of the financial system for the purposes of money laundering and terrorist financing and to lead, coordinate and monitor the AML/CFT efforts of all EU financial services providers and competent authorities. See https://eba.europa.eu/sites/default/documents/files/document_library/News%20and%20Press/Press%20Room/Press%20Releases/2020/EBA%20acts%20to%20improve%20AML/CFT%20supervision%20in%20Europe/AML%20CFT%20Factsheet.pdf.

182 See Articles 9b and 17 of the EBA Regulation. Article 9b(1) of the EBA Regulation states that “In matters concerning the prevention of and countering the use of the financial system for the purposes of money laundering and terrorist financing, in accordance with Directive (EU) 2015/849, the Authority may, where it has indications of material breaches, request a competent authority [...] to investigate possible breaches of Union law”.

183 Article 4(1) of DIRECTIVE (EU) 2017/1371 (PIF Directive), states that “Member States shall take the necessary measures to ensure that money laundering as described in Article 1(3) of Directive (EU) 2015/849 [AMLD 4] involving property derived from the criminal offences covered by this Directive constitutes a criminal offence”. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017L1371&from=EN>.

184 See <https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces>.

- » Shutting down one of the largest cryptocurrency tumblers – “bestmixer”¹⁸⁵ – together with Dutch and Luxembourg authorities.
- » Working with the Spanish police to take-down an organised crime group suspected of operating a VC money-laundering scheme on behalf of other organised crime groups. The intercepted scheme involved two bitcoin ATMs, which the groups used to launder money from drug trafficking, including by exchanging the proceeds into VCs. They then transferred the VCs to other virtual wallets controlled by a Colombian criminal organisation¹⁸⁶.
- » Arresting ten hackers suspected of stealing \$100 million in cryptocurrency in “SIM-swapping”¹⁸⁷ attacks, after an investigation with cooperation from Britain, the U.S., Malta, Belgium, and Canada¹⁸⁸.

This shows the importance of international co-operation in taking down criminal organisations and why strengthening international co-operation is one of the Recommendations from the 4th Global Conference on Criminal Finances and Cryptocurrencies by INTERPOL, EUROPOL and Basel Institute on Governance held on 19 November 2020. The other recommendations are to¹⁸⁹:

- a. Adopt tools to extend capabilities on how to investigate VAs
- b. Apply rules to regulate VASPs to prevent money laundering
- c. Apply the strategy to “Follow the Money”
- d. Adopt a multidisciplinary approach
- e. Promote new technologies applied to the financial investigation on VAs
- f. Adapt investigation strategies

Eurojust

Eurojust is an EU agency composed of 27 national members and focuses on judicial co-operation in criminal matters among the competent authorities of EU Member States. Due to the nature of cross-border crime, Eurojust also co-operates with third states and EU bodies such as the Europol, the European Judicial Network, and the European Anti-fraud Office (“OLAF”). On 12 December 2019, Eurojust became the European Agency for Criminal Justice Cooperation, with Regulation (EU) 2018/1727¹⁹⁰ as the legal basis. Eurojust has supported the national authorities of 15 countries in taking down an organised crime group involved in money laundering¹⁹¹. For example, on 30 January 2020,

185 See <https://www.europol.europa.eu/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down>.

186 See <https://www.europol.europa.eu/newsroom/news/cryptocurrency-laundering-service-members-of-criminal-organisation-arrested-in-spain>.

187 These attacks allowed the suspects to gain access to their victims’ phones. See <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/sim-swapping-%E2%80%93-mobile-phone-scam>.

188 For further information please consult: <https://www.europol.europa.eu/newsroom/news/ten-hackers-arrested-for-string-of-sim-swapping-attacks-against-celebrities>.

189 For further information please consult: <https://www.europol.europa.eu/events/4th-global-conference-criminal-finances-and-cryptocurrencies>.

190 For further information please consult: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1727&from=EN>.

191 For further information please consult: <http://www.eurojust.europa.eu/press/PressReleases/Pages/2019/2019-07-10.aspx>.

Eurojust worked with French and Belgian authorities, with the support of Europol, to take enforcement action against a criminal network which committed large-scale international fraud through the sale of Bitcoin and other VCs¹⁹². European Investigation Orders (“EIOs”)¹⁹³ were issued to the authorities of Bulgaria, Hungary, the United Kingdom, Spain, the Czech Republic, and Portugal to help with the investigations.

E. FUTURE TRENDS TO LOOK OUT FOR

The following trends will continue to gain traction in future months:

- » **“Know your transaction” solutions and forensic tools:** VC investigations are nowadays partly supported by commercial (e.g., Chainalysis, Elliptic, CipherTrace, Netki, TRM Labs, etc.) tools and services. As money laundering regulations become more stringent, many companies are turning to blockchain forensics tools and transaction monitoring services. This enables companies to see how many funds have moved from one wallet to another and monitor transactions executed on behalf of their customers to help identify any potential suspicious or unusual transactions that indicate a risk of money laundering. This will ultimately allow the company to understand what risk each and every VC holder presents. Shapeshift, a decentralised exchange, published a blog post in 2019 describing how it handles law enforcement compliance requests¹⁹⁴. Interestingly, half of the requests it received in 2019 were by EU member states. Even on the U.S. centralised exchange, Kraken, EU member states account for about one quarter of requests¹⁹⁵. Both the number of requests and the fact that exchanges publish such information pertaining to requests indicate that the VC world takes compliance with law enforcement seriously.
- » **RegTech¹⁹⁶ and SupTech¹⁹⁷:** regulatory technology (“RegTech”) is the use of technological solutions for regulatory process compliance within the financial and fintech industries. For example, most KYC processes require individuals to provide personal data for identity verification. However, since the *General Data Protection Regulation (EU) 2016/679 (GDPR)* came into force, fintech companies have been forced to create new mechanisms for storing and processing such personal data. Under the coordination of the ECB, the European System of Central Banks (“ESCB”) and the EUROchain¹⁹⁸ research network has set up a proof of concept for a central bank digital token that would offer some anonymity (i.e., the option to keep a user’s identity and transaction history hidden) between central banks and users, while also monitoring the transactions and automating limits on anonymous transactions to help intercept tax evasion, offshore accounts,

192 For further information please consult: <http://www.eurojust.europa.eu/press/PressReleases/Pages/2020/2020-01-30.aspx>

193 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters. Article 1(1) of the Directive states that a EIO is “a judicial decision which has been issued or validated by a judicial authority of a Member State (‘the issuing State’) to have one or several specific investigative measure(s) carried out in another Member State (‘the executing State’) to obtain evidence in accordance with this Directive. The EIO may also be issued for obtaining evidence that is already in the possession of the competent authorities of the executing State”.

194 For further information please consult: <https://info.shapeshift.io/blog/2019/01/18/pulling-back-the-curtain-how-shapeshift-handles-law-enforcement-compliance/>.

195 For further information please consult: <https://cointelegraph.com/news/law-enforcement-requests-to-kraken-hit-all-time-high-up-49-in-2019>.

196 Primavera De Filippi and Aaron Wright. (2018) *Blockchain and the Law*. Pp. 193-204.

197 SupTech (supervisory technology) is defined by the Bank for International Settlements (BIS) as “the use of innovative technology by supervisory agencies to support supervision”.

198 For more information please consult: <https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf>.

money laundering, accounting tricks, and the movement of dirty money. Technical solutions like these help with being GDPR and AMLD5 compliant while also limiting anonymity, a key objective of AMLD5.

- » **Seizure & Auctions:** Similar to when the proceeds of money laundering are seized, authorities have had to grapple with what to do when wallets are frozen or VCs are seized. The December 2019 Eurojust “Cybercrime Judicial Monitor” report – Issue 5, which is based on information provided by the European Judicial Cybercrime Network, states that “[m]ost countries do not have any specific (criminal) legal provisions on virtual currencies and apply general provisions of criminal law on seizure and asset recovery or anti-money laundering and terrorism financing laws”. In most countries, the seized virtual currencies are transferred to law enforcement authority wallets. In Ireland, the independent auctioneer “Wilsons Auctions” has hosted several cryptocurrency auctions¹⁹⁹ and on 24 March 2020 Wilsons Auctions Ireland was scheduled to help Belgium sell over EUR 110,000 worth of bitcoin and cryptocurrency seized by the Belgian government²⁰⁰. This could indicate a future trend for the rest of Europe²⁰¹.
- » **VC crime insurance:** Insurance brokers are starting to offer crime insurance to institutions for cold and hot wallets. Policies can cover losses on everything from natural disasters that destroy the private keys under custodianship in hardware wallets to hot wallets that are hacked²⁰². Whether insurance brokers will insure companies that do not have robust AMLD5 policies in place will also be something to look out for.

F. QUO VADIS?

Further reflection is required on what to do as the technology used by criminals outpaces the legislation (e.g., “crypto dusting” is a type of blockchain spam that sends digital tokens to a large group of addresses and thereby taints addresses by making them transact with mixers without their consent). The 2018 study commissioned by the European Parliament, entitled “Virtual currencies and terrorist financing: assessing the risks and evaluating responses” states that:

[B]ecause the emphasis of regulatory regimes to date has been on placing oversight where users interact with centralised third-party gatekeepers, it remains unclear whether the regulatory regime as set out in the 5AMLD will remain relevant in the face of a growing range of DEXs, atomic swaps and other P2P applications that may sit outside the historical paradigm of the AML/CFT regime.

199 For more information please consult: <https://cointelegraph.com/news/belgian-govt-will-sell-125k-of-seized-bitcoin-in-irish-public-auction> and <https://cointelegraph.com/news/crypto-auctions-where-do-arrested-bitcoins-end-up>.

200 For more information please consult: <https://www.wilsonsauctions.com/news/wilsons-auctions-to-host-first-public-cryptocurrency-auction-in-ireland/>. Chainalysis has also launched a new program to help governments sell seized virtual currencies, See <https://news.bitcoin.com/chainalysis-launches-program-to-store-and-sell-seized-crypto-assets-for-governments/>

201 It has been suggested that reserve funds could be created instead of auctioning off virtual currencies, however this is unlikely to gain traction given the fact that governments do not currently want exposure to decentralized virtual currencies like bitcoin. See <https://pierre-rochard.medium.com/urgent-bitcoin-legislation-4e715b7864d2>.

202 For more information please consult: e.g., <https://www.coindesk.com/aon-metaco-crypto-custody-insurance>; <https://www.coindesk.com/bitstamp-adds-crypto-crime-insurance-for-assets-held-online>; and <https://cointelegraph.com/news/ledger-vault-secures-150-million-crime-insurance-policy-for-digital-assets>

VII. Conclusion

Any innovation comes with a discussion on whether, and to what extent, the activity should be specifically regulated or falls within existing regulation. In order to better encounter for the opportunities and risks that digital tokens may have embedded, European Union institutions have declared that they “are committed to put in place the framework that will harness the potential opportunities that some digital tokens may offer”²⁰³. Opportunities are not exempt of risk, so the legislative action needs to act carefully in order to strike the right balances. Throughout this report we have had the opportunity to explore the current state of affairs in terms of legislation applicable to tokens in the EU and pointed at some potential gaps yet to be solved.

From a financial law perspective, despite the new legislation proposed can serve as a good start to create a uniform framework for digital tokens in the EU, there is still a long way ahead. For starters, the proposed regulations might never be enacted and even if they are someday, its content might be outdated by then at the pace innovation occurs in the DLT ecosystem. There is also room for action in providing useful, stable guidance on how existing legislation applies to digital tokens, to ensure it is clear for market participants when they are subject to the financial legislation package or to the MiCA Regulation Proposal regime, if enacted. This is especially true for stablecoins, as it might be challenging to define when they function as financial instruments or as e-money or asset-referenced tokens instead. In addition, it is yet to be seen if the EC will put in place targeted legislative changes removing provisions acting as a barrier to issuance, trading and post-trading of Securities tokens.

From a tax law perspective, the current lack of harmonization in terms of classification and applicable tax regimes leaves national tax authorities with large discretion in order to interpret the characteristics of various tokens, leaving a risk of similar cases not being treated similar, or also the other way around where different cases are treated similar as a matter of simplification. This may lead to uncertainty and potentially double taxation as well if digital tokens are not included in bilateral tax agreements. Even though it can be argued that harmonization at both regional and global scale would be beneficial for any cross-border activity, there are a number of constraints in order to reach satisfactory compromises in this regard. This is true for agreeing on a commonly recognized taxonomy for token classification, let alone common tax principles. A question in this regard is whether, and the extent to which, already existing international agreements on tax collaboration and exchange of information applies for holdings of digital tokens. Most probably, there is a need to include specific details in the already existing agreements in this regard, including coming up with a common framework for token classification in order to know what kind of information authorities from other jurisdictions can receive upon request.

Despite promising initiatives towards more regulatory harmonization of digital tokens in Europe, it is safe to expect that taxation of digital tokens will rest with domestic legislators to decide for a long time. This means that we will have to grapple with regulatory fragmentation in the domain of digital tokens, where legal hybrids will have to be monitored by domestic tax authorities.

²⁰³ Joint Statement of the European Commission and Council on stablecoins, 5 December 2019.

From an AML law perspective, as the national laws of EU member states set forth more stringent criteria than AMLD5 and AMLD6, discussions will increase around more harmonisation through a 7th anti-money laundering directive²⁰⁴ in line with the FATF Recommendations or an EU regulation²⁰⁵. As AMLD5 sets out to limit the risks presented by the cross border-nature of digital token transactions, co-operation will be key. Statements by European bodies indicate that the trend will be towards more co-ordination and supervisory convergence at the European level.

204 AMLD6 (Sixth Anti-money Laundering Directive) is the 2018/1673 Directive of the European Union and was adopted on 12 November 2018 and must be implemented by EU member states by no later than 3 December 2020. It does not add anything new to the topic of VCs, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1673&from=EN>.

205 See para. 18 of 5 December 2019 Council conclusions on strategic priorities on anti-money laundering and countering the financing of terrorism, as adopted by the Council (ECOFIN) at its 3736th meeting held on in Brussels, <http://data.consilium.europa.eu/doc/document/ST-14823-2019-INIT/en/pdf>. See also 26 February 2020 "Banking Union - annual report 2019" https://www.europarl.europa.eu/doceo/document/A-9-2020-0026_EN.html. Section 38 of the report "welcomes the joint position paper of 8 November, prepared by several euro area finance ministers, which calls for the harmonisation of the European money laundering and terrorism financing regulatory framework". On 8 November 2019, the Dutch Minister of Finance sent a joint position paper to the Dutch Parliament regarding the need for a European AML supervisor (Anti-money laundering). The paper was prepared by the Ministers of Finance of Germany, France, Italy, Spain, Latvia, and the Netherlands. See p. 2 of the joint position paper for the mention of an AML regulation, as opposed to a directive. See <https://www.rijksoverheid.nl/documenten/kamerstukken/2019/11/08/position-paper>.

Abbreviations (in order of appearance)

EU - European Union

DLT - Distributed Ledger Technology

ESMA - European Securities and Markets Authority

EBA - European Banking Authority

EC - European Commission

ICO - Initial Coin Offering

ESMA Report - *Advice Initial Coin Offerings and Crypto-Assets*

EBA Report - *Report with advice for the European Commission on crypto-assets*

EC Consultation - *Consultation Document on an EU framework for markets in crypto-assets*

AMLD5 - 5th Anti-Money Laundering Directive (Directive 2018/843/EU)

MIFID2 - Markets in Financial Instruments Directive II (2014/65/EU)

EMD2 - Electronic Money Directive (2009/110/EC)

FAFT - Financial Action Task Force

FCA - Financial Conduct Authority

ECB - European Central Bank

FCA Report - *Guidance on Cryptoassets*

EACB - European Association of Cooperative Banks

EACB Response - *EACB response to the EC's Online Public Consultation on an EU framework for markets in crypto-assets*

FMLC - Financial Markets Law Committee

PSD2 - Payment Services Directive

PR - Prospectus Regulation

AMF - *Autorite Des Marches Financiers*

MiFIR - Markets in Financial Instruments Regulation (600/2014/EU)

MAR - Market Abuse Regulation (596/2014/EU)

SSR - Short Selling Regulation (236/2012/EU)

CSDR - Central Securities Depositories Regulation (909/2014/EU)

SFD - Settlement Finality Directive (98/26/EC)

EMIR - European Markets Infrastructure Regulation (648/2012/EU)

FCD - Financial Collateral Directive (2002/47/EC)

AIFMD - Alternative Investment Fund Managers Directive (2011/61/EU)

UCITS Directive – Undertaking for Collective Investment in Transferable Securities Directive (2009/65/EC)

CRD – Capital Requirements Directive (2013/36/EU)

CRR – Capital Requirements Regulation (2013/575/EU)

MTF – Multilateral Trading Facility

OTF – Organized Trading Facility

G7 Report – *Investigating the impact of global stablecoins*

STO – Securities Token Offering

WFE – World Federation of Exchanges

SMSG – Securities and Markets Stakeholders Group

CFTC – Commodity Futures Trading Commission

FSB – Financial Stability Board

BCBS – Committee on Banking Supervision

OECD – Organisation for Economic Co-operation and Development

DeFi – Decentralised Finance

EBSI – European Blockchain Services Infrastructure

VASPs – Virtual Asset Service Providers

VC – Virtual currency, under the meaning of AMLD5 (see Section IV(B)(1))

AML/CFT – Anti-money laundering and combatting the financing of terrorism

VA – Virtual asset, as defined by the FAFT (see Section IV(B)(1))

VC exchanges – Providers engaged in exchange services between virtual currencies and fiat currencies

CDD – Customer due diligence checks

2019 Guidance – *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*

EPPO – European Public Prosecutor’s Office

Europol – EU Agency for Law Enforcement Cooperation

Definitions (in order of appearance)

Digital token or token: For the purpose of this report, digital tokens or tokens are transferable units generated within a distributed network that tracks ownership of the units through the application of blockchain technology.

Crypto-asset: For the purpose of this report, crypto-asset means a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology, in line with Article 3(1)(2) of the MiCA Regulation Proposal.

Securities token: For the purpose of this report, Securities tokens are a type of digital tokens that qualify as a financial instrument under MiFID2 (see Section II(B) of this report).

DLT Transferable securities: For the purpose of this report, DLT transferable securities means transferable securities within the meaning of Article 4(1)(44) (a) and (b) of Directive 2014/65/EU that are issued, recorded, transferred and stored using a DLT.

Utility token: For the purpose of this report, utility tokens means a type of crypto-asset which is intended to provide digital access to a good or service, available on DLT, and is only accepted by the issuer of that token, in line with Article 3(1)(5) of the MiCA Regulation Proposal.

E-money token: For the purpose of this report, means a type of crypto-asset the main purpose of which is to be used as a means of exchange and that purports to maintain a stable value by referring to the value of a fiat currency that is legal tender, in line with Article 3(1)(3) of the MiCA Regulation Proposal.

Asset-referenced token: For the purposes of this report, asset-referenced token means a type of crypto-asset that purports to maintain a stable value by referring to the value of several fiat currencies that are legal tender, one or several commodities or one or several crypto-assets, or a combination of such assets, in line with Article 3(1)(5) of the MiCA Regulation Proposal.

Payment token: For the purpose of this report, payment tokens are a type of digital tokens that may serve as a means of payment or exchange.

Investment token: For the purpose of this report, investment tokens are a type of digital token with profit-rights attached to it.

Electronic money or e-money: Electronic money means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer.

Financial instrument: Those instruments specified in Section C of Annex I in MiFID2. (see Section II(B) of this report).

Payment service: Any business activity set out in Annex I of PSD2.

Funds: means banknotes and coins, scriptural money or electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC.

Transferable security: For the purposes of this report, transferable securities mean those classes of securities which are negotiable on the capital markets in line with Article 4(1)(44) MiFID2.

Chargeable event: occurrence by virtue of which the legal conditions necessary for VAT to become chargeable are fulfilled.

Trading venue: A regulated market, or MTF or OTF under MiFID2.

Qualified investors: For the purposes of this report, the term “qualified investors” means professional clients under MiFID2.

Professional client: Client who possesses the experience, knowledge, and expertise to make its own investment decisions and properly assess the risks that it incurs. In order to be considered to be professional client, the client must comply with the criteria laid down in Annex II of MiFID2.

Multilateral system: Any system or facility in which multiple third-party buying and selling trading interests in financial instruments are able to interact in the system.

Regulated market: Multilateral system operated and/or managed by a market operator, which brings together or facilitates the bringing together of multiple third-party buying and selling interests in financial instruments – in the system and in accordance with its non-discretionary rules – in a way that results in a contract, in respect of the financial instruments admitted to trading under its rules and/or systems, and which is authorised and functions regularly and in accordance with Title III of MiFID2.

Multilateral trading facility: Multilateral system, operated by an investment firm or a market operator, which brings together multiple third-party buying and selling interests in financial instruments – in the system and in accordance with non-discretionary rules – in a way that results in a contract in accordance with Title II of MiFID2.

Organized trading facility: Multilateral system which is not a regulated market or an MTF and in which multiple third-party buying and selling interests in bonds, structured finance products, emission allowances or derivatives are able to interact in the system in a way that results in a contract in accordance with Title II of MiFID2.

Airdrop: Event where holders of tokens receive new tokens due the initial ownership.

Virtual currency: Under AMLD5, virtual currency means 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”.

Virtual asset: Digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations.

Obligated entities: Any entity listed in Article 2(1) of the AML4.



UNDERSTANDING DIGITAL TOKENS

**Legal Landscapes Governing Digital
Tokens in the European Union**