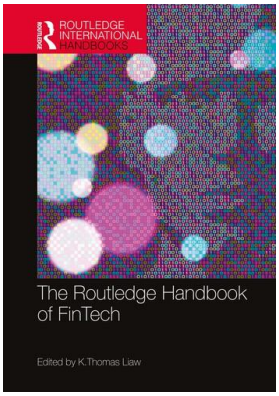

The Routledge Handbook of FinTech

K. Thomas

Cryptoassets and financial crime

Publication details
https://test.routledgehandbooks.com/doi/10.4324/9780429292903-13
Robby Houben, Alexander Snyers
Published online on: 15 Jun 2021

11

CRYPTOASSETS AND FINANCIAL CRIME

A European Union perspective

Robby Houben and Alexander Snyers

I Introduction

At the start of 2020, over 5,100 cryptoassets existed with a total market capitalisation exceeding $250 billion.[1] Cryptoassets can be used both for legal and illegal purposes. Most legal activity in cryptoassets – and in particular in cryptocurrencies – takes place on crypto-exchanges and relates to the use of cryptocurrencies as an investment.[2] For illegal purposes cryptocurrencies are used mostly as a means of payment, e.g., to buy or sell of illegal goods or services, launder money, finance terrorism or evade capital controls. Remarkable is that almost half of all (yearly) transactions in Bitcoin can be linked to illegal activity, amounting to approximately US$76 billion of illegal activity per year involving Bitcoin; a number that comes very close to the US and EU markets for illegal drugs.[3] As the crypto-market is still dominated by Bitcoin, with a dominance in terms of total market capitalisation exceeding 63% ($159 billion), [4] this is an important observation.

The market capitalisation of privacy/anonymity-enhancing coins like Monero (XMR) and Dash (DASH)[5] declined significantly at the end of 2018 and over the course of 2019. However, these coins remain popular, staying in the top 20 of coins in terms of market capitalisation, with daily trading volumes exceeding several million US dollars.[6] Hence, despite the availability on the market of privacy/anonymity-enhancing coins like Dash and Monero, Bitcoin is still king[7]: illegal users apparently keep resorting to third-party privacy/anonymity-enhancing services like mixers and tumblers (which obfuscate both the identifies of the sender and recipient of a coin) to conceal their crypto-transactions, rather than shift their focus entirely to privacy/anonymity-enhancing coins.

This chapter scrutinizes the use of cryptoassets in the context of financial crime and regulatory responses in the European Union (EU).

The chapter takes a legal perspective. We will not elaborate on the technical aspects relating to cryptoassets, unless that is necessary to understand the legal context. We will also not take an economic, criminological or any other approach than a legal one.

The focus is on the EU legal context. We will elaborate on the international[8] or national context only if relevant to better understand the European context.

The research relates to the use of cryptoassets in the context of financial crime. Financial crime is no term of art. Generally speaking, it is used as an umbrella term to designate

all sorts of crimes relating to the use of finances, such as fraud, theft, tax evasion, bribery, money laundering, terrorist financing, etc. In an EU context, financial crime includes *inter alia* crimes against the integrity of the financial sector, such as money laundering and insider dealing, and crimes against the financial interest of the Union, such as fraud. This chapter will not elaborate on all imaginable financial crimes, yet will focus on money laundering and terrorist financing as subtypes of financial crime. This focus can be justified for a number of reasons. Firstly, money laundering and terrorist financing are at the forefront of the EU's efforts on combating financial crime.[9] Furthermore, the EU is clearly taking the approach to address cryptocurrency issues via anti-money laundering and counter terrorism financing legislation[10]. Thirdly, leaving theft and tax evasion aside, money laundering and terrorist financing are probably the two types of financial crimes that are likely to be most associated with cryptoassets. Cryptoassets are thought to be very suitable for money laundering and terrorist financing because they are assets that are fully digital, easily transferable, decentralised, cross-border, pseudonymous[11] – and with the use of specific anonymity-enhancing technology even completely anonymous.[12]

We will not discuss other legal queries than those related to financial crime, such as the qualification of cryptocurrencies under tax laws, the protection of investors in cryptoassets (whether or not consumers) under financial services laws, the prudential treatment of crypto- on a financial institution's balance sheet or the impact of cryptoassets on monetary policy and financial stability.

We start by assessing what exactly cryptoassets are. Secondly, we identify the key actors in cryptoasset schemes. Thirdly, the challenges cryptoassets bring from the perspective of combating financial crime are scrutinised. Subsequently the EU regulatory framework relating to money laundering and terrorist financing via cryptoassets is critically assessed and suggestions for future law-making are made. The chapter concludes with a brief note on cybersecurity and some thoughts on the right level of law-making as regards cryptoassets.

II What are cryptoassets?

A A wide variety of assets

In recent years the crypto-market has changed significantly. Amongst the most notable recent developments are the massive growth of the number of so-called private "tokens" issued on existing platforms in order to raise funds, and the emergence of so-called "stablecoins" and central bank digital currencies (CBDCs). These trends have caused various regulatory authorities, standard-setting bodies and legal scholars to shift their focus and expand their vocabulary from the term "cryptocurrencies" to the broader term "cryptoassets".[13]

At present, the term "cryptoassets" is used to refer to a wide variety of assets. Despite its frequent use, there is no generally accepted definition of what constitutes a cryptoasset.[14] Different definitions have been adopted by regulatory authorities and standard-setting bodies.[15] This chapter builds further on the definition of the European Banking Authority (EBA)[16] and defines a cryptoasset as a private digital asset that:

- is recorded on some form of a digital distributed ledger secured with cryptography;
- is neither issued nor guaranteed by a central bank or public authority; and
- can be used as a means of exchange and/or for investment purposes and/or to access a good or service.[17]

B Summa divisio: *cryptocurrencies and tokens*

Cryptoassets can take on different forms and have various characteristics.[18] From a bird's eye view, a *summa divisio* can be made between cryptocurrencies and tokens.

Cryptocurrencies (or coins), such as Bitcoin, are cryptoassets that are designed or intended to perform the roles of currency, *i.e.* to function as a general-purpose medium of exchange, a store of value and a unit of account.[19] They are intended to constitute a peer-to-peer alternative to government-issued legal tender.[20]

Tokens, on the other hand, are cryptoassets that offer their holders certain economic and/or governance and/or utility/consumption rights.[21] Broadly speaking, they are digital representations of interests, or rights to (access) certain assets, products or services.[22] Tokens are typically issued on an existing platform or blockchain to raise capital for new entrepreneurial projects, or to fund start-ups or the development of new (technologically) innovative services.[23]

Cryptocurrencies were the first type of cryptoassets to emerge, with the creation of Bitcoin already dating back from late 2008 to early 2009.[24] Tokens, which are the result of a transaction carried out by an issuer, generally in connection with the collection of financial resources,[25] became widely popular by the end of 2017; a trend that persists until this day. They are, what could be called, the second generation of cryptoassets.

Broadly speaking, there are two categories of tokens: investment tokens and utility tokens.[26]

Investment tokens – sometimes also referred to as security tokens or asset tokens – are tokens that typically provide their holders rights in the form of ownership rights and/or entitlements that are similar to dividends.[27] Investment tokens are generally issued for the purpose of capital raising (*i.e.* through an ICO[28]) and show similarities to traditional debt and equity instruments.[29] In addition, the term "investment token" is also used to refer to traditional securities or other assets that have undergone the process of tokenisation (*i.e.* that have been registered on a blockchain in the form of a token).[30]

Utility tokens are tokens that grant their holders access to a specific application, product or service often provided through a newly developed (blockchain-type) infrastructure.[31] They typically only provide access to a product or service developed by the token issuer and are not accepted as a means of payment for other products or services.[32] Hence, they differ from cryptocurrencies. Like investment tokens, utility tokens are also issued to collect financial resources, usually to fund the further development of the issuer's application, product or service. However, unlike investment tokens, their main purpose is not to generate future cash flows for investors, but to grant access to the issuer's application, product or service, [33] and at the same time create a user base. The value of utility tokens is typically derived from their functional component.[34]

While it is theoretically feasible to draw a clear dividing line between cryptocurrencies and tokens, and, within the latter category, investment and utility tokens, in practice it is not always easy to fit a cryptoasset into one or the other category.[35] This is because cryptoassets can exhibit features of more than one (sub-)category: they can embody a combination of an investment and/or a utility and/or a payment function. Cryptoassets that embody such a combination are commonly referred to as "hybrids" or "hybrid tokens"[36] and raise particular regulatory challenges, especially in the context of crypto investor protection.

C Central bank digital currencies

The emergence, and growing popularity, of cryptocurrencies and their underlying technology have inspired various central banks to investigate whether it would make sense for

them to issue their own "digital currencies", for wholesale purposes, or as a complement to or a substitute for physical banknotes and coins.[37] These digital currencies, the advent of which is still largely theoretical,[38] are commonly referred to as central bank digital currencies (CBDCs).[39] Simply put, a CBDC is a digital asset or a digitalised instrument issued by a central bank for the purpose of payment and settlement, in either retail or wholesale transactions.[40] Since it is issued by a central bank, and is a central bank liability, it could be described as a sovereign coin.

CBDCs could have diverse benefits, yet at the same time, also raise various (monetary policy) concerns. Like cryptocurrencies, which are at the very least intended to perform the roles of currency, CBDCs are digital currencies. However, that is as far as the comparison goes. Whereas cryptocurrencies, a subcategory of cryptoassets, are private in nature, generally make use of some form of distributed ledger technology (DLT) and are not issued or guaranteed by a central bank, the opposite is true for CBDCs.[41] A clear dividing line between cryptocurrencies, or even broader, cryptoassets, on the one hand, and CBDCs on the other hand, should therefore be drawn.

D Stablecoins

The first wave of cryptocurrencies, which began with Bitcoin and hundreds of subsequent Bitcoin clones,[42] are considered by their users as "something of value". They do not represent any underlying asset, claim or liability,[43] making them prone to high price volatility.[44] They are what could be called traditional "non-backed" cryptocurrencies.

The highly volatile nature of traditional "non-backed" cryptocurrencies makes it very hard for them to truly perform the roles of currency (*i.e.* function as a medium of exchange, a store of value and a unit of account) and to become more widely adopted as such.[45] In view hereof, central banks usually refrain from using the term crypto*currencies* to refer to these cryptoassets all-together.[46]

A number of cryptocurrency advocates have recognised that the severe price volatility of the first wave of cryptocurrencies is indeed a major hurdle for their acceptance as a means of payment and store of value. They have tried to address the issue at hand by introducing so-called stablecoins.[47] Simply put, a stablecoin is a variant or subcategory of cryptocurrencies typically pegged or linked to the price of another asset or a pool of assets, designed to maintain a stable value.[48] Like traditional "non-backed" cryptocurrencies, stablecoins are intended to perform the roles of currency. Unlike traditional "non-backed" cryptocurrencies, which are generally decentralised,[49] and do not have an identifiable issuer or at least not an institution that can easily be held accountable by or towards the coin's users, stablecoins typically represent a "claim" on a specific issuer or on underlying assets or funds, or some other right or interest.[50] They are, in other words, backed by something and not just perceived to be "something of value".

Stablecoins share a number of properties with "tokens" and are sometimes even identified as such.[51] Like tokens, stablecoins are typically issued on an existing blockchain and embody a claim (*vis-à-vis* an identifiable issuer or on assets backing the coins). However, whereas tokens are issued with a very specific functionality or for a specific purpose (e.g., to provide their holders ownership rights and/or dividend-like rights, or to enable access to a specific product or service), [52] stablecoins generally lack such functionality. They are intended to be used as a general-purpose medium of exchange: to enable the buying and selling of a good or service provided by someone other than the issuer. Therefore, they should be distinguished from tokens, rather than be identified as such.

Although most stablecoins can be traded on one or more crypto-exchanges on a 24/7 basis, from nearly anywhere in the world, they have yet to reach a very wide user base. Their actual footprint usually does not reach further than a few jurisdictions. In other words, their impact remains rather local. Recently, however, new stablecoin initiatives have emerged. Most important is probably Facebook's Libra project (recently renamed the Diem project). These new initiatives are built on top of existing, large and/or cross-border user bases. Therefore, they have the potential to scale very quickly to achieve a global or other substantial footprint[53] and are, as a result, commonly referred to as "global stablecoins".[54] Global stablecoins are currently under a lot of scrutiny, because they could pose significant risks to financial stability and monetary policy.

E Initial coin offerings: coins or tokens issued by an identifiable issuer

To conclude our introduction on cryptoassets, it is relevant to briefly concentrate on initial coin offerings (ICOs).

In the beginning, the term ICO was primarily used to refer to a crowdsale organised upon the launch of a new cryptocurrency by a known or identifiable issuer.[55] The coin's inventors pre-mined a number of coins and offered them to the public through a crowdsale to pay for development costs.[56]

Today, the term ICO is commonly used by regulatory authorities and legal scholars to refer to a process in which businesses (usually start-ups) or individuals issue tokens to the public to raise funds for their projects, in exchange for fiat money or other cryptoassets.[57] In legal literature, ICOs are typically compared to initial public offerings (IPOs). Both are commonly referred to with three-letter acronyms and both are aimed at raising money from the general public. There are, however, a number of differences between the two, aside from the instruments issued. Firstly, whereas a successful IPO generally requires the issuing companies to have a certain track-record, a successful ICO can be initiated at any stage. Secondly, IPOs typically involve a costly and time-consuming process. ICOs, on the other hand, can be launched through the issuer's website in a short period of time and generally do not require multiple actions from traditional intermediaries.[58]

An ICO is typically preceded by a so-called "white-paper" made available on the issuer's website, in which the issuer describes their project, the tokens that will be issued and the technology and protocols underlying them.[59] The issuer will subsequently announce their project to the general public along with the date of the ICO through social media.[60] In order to subscribe to, hold and – at a later stage – trade tokens, investors will need to acquire a "digital wallet".[61] Such wallet is also required to store and exchange other cryptoassets.

As indicated on p. 164–165, the words "initial coin offering" are currently used in a dual context to refer both to coins (cryptocurrencies) and tokens issued by an identifiable issuer. This is confusing. It makes sense to henceforth use the words "initial cryptoasset offering", which can also be abbreviated with the acronym ICO.[62]

It is important to note that not all cryptoassets, especially decentralised cryptocurrencies, have an identifiable issuer. The most important example is Bitcoin: Bitcoin is not issued by or under supervision of a central authority and no central authority is required to verify Bitcoin transactions.

III Key actors in cryptoasset schemes

Hereinafter we give a brief overview of the key actors in cryptoasset schemes, without trying to be exhaustive. The overview is relevant to draw conclusions with respect to the EU regulatory framework on money laundering and terrorist financing via cryptoassets.

The following actors can be distinguished:

- **users** – users are persons using cryptoassets, mainly to pay for goods or services or to speculate; users include, e.g., traders, suppliers or customers;
- **miners**[63] – miners participate in the validation of transactions on the blockchain by solving a "cryptographic puzzle" and are rewarded with newly mined coins;[64]
- **crypto exchanges**[65] – crypto exchanges offer exchange services to cryptoasset users. Some exchanges are pure crypto exchanges and accept only payments in other cryptocurrencies, usually Bitcoin, whereas others also accept payments in fiat currencies such as US dollar or euro;
- **trading platforms**[66] – trading platforms are online market places where cryptoasset users can post bids and offers and, as a result, transact with each other. Some trading platforms facilitate trades as an intermediary, whereas others operate on a decentralised basis: they are not run by an entity that oversees and processes all trades, but are operated exclusively by software.
- **wallet providers**[67] – wallet providers are entities that provide cryptoasset users with digital wallets that are used for holding, storing and transferring cryptoassets. There are several types of wallet providers:
  - hardware wallet providers that provide cryptoasset users with specific hardware solutions to privately store their cryptographic keys;
  - software wallet providers that provide cryptoasset users with software applications which allow them to access the network, send and receive cryptoassets and locally save their cryptographic keys; and
  - custodian wallet providers that take (online) custody of a cryptoasset user's cryptographic keys.
- **cryptoasset creators** – cryptoasset creators are persons who have developed the technical foundations of a cryptoasset and have set the initial rules for its use. In some cases their identity is known (e.g., Ripple or, the yet to be launched, Libra (Diem coin)), but every so often they remain unidentified (e.g., Bitcoin, Monero).
- **cryptoasset issuers** – cryptoasset issuers are persons who offer cryptoassets to users upon the cryptoasset's initial release. Not all cryptoassets, especially cryptocurrencies, have an identifiable issuer; tokens, on the other hand, mostly do.[68]
- **cryptoasset "financial services"**[69] **providers** – cryptoasset "financial services" providers are persons providing "financial services" in respect of cryptoassets after the asset's initial release, e.g., cryptoasset brokers or cryptoasset agents.

IV Key challenges in the fight against money laundering and terrorist financing via cryptoassets

Taking into account the definition of cryptoassets and the identified key actors in cryptoasset schemes, the key issue that needs to be addressed in order to adequately capture cryptoassets and cryptoasset actors in legislation is to unveil the anonymity, varying from pseudo-anonymity to complete anonymity, which surrounds them. This anonymity prevents cryptoasset transactions from being adequately monitored, allowing shady transactions to occur outside of the regulatory perimeter and allowing criminal organisations to use cryptoassets to obtain easy access to "clean cash" (both cash in and cash out).

Introducing regulation that unveils anonymity of course invokes the privacy question. In this respect, a balance should be struck between preserving strong encryption for the protection of cybersecurity, data protection and privacy on the one hand and offering opportunities for legitimate law enforcement to obtain access to information for the purpose of criminal investigations with appropriate safeguards on the other hand.[70]

In addition to anonymity, the intrinsically cross-border nature of cryptoassets, crypto-markets and crypto-actors is a major challenge for regulators.[71] One of the issues is, for instance, that crypto-markets and crypto-actors can be located in jurisdictions that do not have effective money laundering and terrorist financing controls in place.[72] The cross-border nature of cryptoassets, crypto-markets and crypto-actors means that rules will only be adequate when they are taken at a sufficiently international level.[73]

A third challenge is that sometimes there is no central intermediary, such as an issuer, that would normally be the focal point of regulation. Therefore, an important question is to which players in the crypto-market should regulation be attached, absent a central intermediary?[74] A line of thought for future regulation could here be to create or impose a "middleman", where the use of blockchain or other distributed ledger technology has cut out such middleman, as this will allow the regulator to attach regulation to an identifiable person, thus contributing to enhanced compliance and effective enforcement. But, of course, such approach would stand in sharp contrast with what the early day, decentralised cryptocurrencies essentially stand for: basically, cutting out the middleman because of distrust in that middleman. Hence, addressing this issue boils down to a trade-off between effective regulation and financial innovation and striking the right balance between these two.

V The existing EU framework deals poorly with these challenges

A Introduction to the EU regime regarding money laundering and terrorist financing

The fight against money laundering and terrorist financing is a key priority of the international community, including the EU. It has long been established that money laundering activities are usually carried out in an international context and that, therefore, national measures are not sufficient. The Recommendations of the Financial Action Task Force (FATF) – drawn up in 1990 and revised from time to time – are the cornerstone of the international framework for combating money laundering and terrorist financing. They have been endorsed by over 180 countries, and are universally recognised as setting out the international standards.

The EU adopted its first Anti-Money Laundering Directive on 10 June 1991.[75] Since then, the EU framework on money laundering has been amended from time to time: a second (in 2001),[76] third (in 2005),[77] fourth (in 2015)[78] and fifth (in 2018)[79] Directive followed, gradually also targeting terrorist financing.

The core principle of the EU framework on money laundering and terrorist financing (hereinafter also referred to as AML/CFT) is the prohibition of money laundering and terrorist financing. In simple terms money laundering can be explained as the process by which proceeds of criminal activity are "cleaned" and brought into the lawful economy so that their illegal origins are concealed or disguised.[80] A difference between terrorist financing and money laundering is that in the event of terrorist financing, the origin of the funds can be legitimate. It is the destination of the funds, *i.e.* financing terrorists, that makes the whole deal illegitimate.[81]

An important building block of AML/CFT legislation are the gatekeepers, technically referred to as "obliged entities". These obliged entities are the entry-point for anti-money laundering and counter terrorism requirements.[82] Typical gatekeepers are credit institutions, financial institutions, a well-defined list of natural or legal persons acting in the exercise of their professional activities (under which auditors, external accountants, tax advisors, notaries and other independent legal professionals), trust or company service providers, estate agents, other persons trading in goods to the extent that payments are made or received in cash in an amount of €10.000 or more and providers of gambling services.[83] The gatekeepers' task essentially is to monitor that their clients comply with criminal laws. To that end, they have to perform customer due diligence checks and report suspicious transactions to the competent financial intelligence unit, among various other rules that are all in similar vein.

B Cryptoassets and the current EU AML/CFT framework

Up until the fifth revision, the EU AML/CFT framework did not include any crypto-assets gatekeeper, *de facto*[84] exempting crypto-activity completely from the scope of AML/CFT legislation. The fifth revision of the AML/CFT framework (hereinafter referred to as AMLD5), however, changed the tide and included measures to pull cryptocurrencies and (some) crypto-actors out of the regulatory dark. Member States were supposed to transpose AMLD5 in their national AML/CFT legislation by 10 January 2020.[85]

Interesting to note is that the EU took the policy choice to address cryptocurrencies and crypto-actors solely via the rules on money laundering and terrorist financing. From a conceptual perspective, there were also other options, e.g., introducing tailored financial services legislation. This would have also pulled cryptocurrencies and cryptoasset actors out of the dark, and even more, e.g., relevant crypto-actors would have needed a license. However, this option, from a policy perspective, was not preferred at this stage.[86]

To address the money laundering and terrorist financing risks presented by cryptocurrencies, AMLD5 included so-called custodian wallet providers (defined as entities that provide services to safeguard private cryptographic keys on behalf of their customers, to hold, store and transfer virtual currencies)[87] and virtual currency exchanges (defined as providers engaged in exchange services between virtual currencies and fiat currencies) in the scope of the EU AML/CFT framework by defining them as obliged entities. As obliged entities, custodian wallet providers and virtual currency exchanges have to comply with the same AML/CFT requirements as banks and other financial institutions, including performing customer due diligence checks and reporting suspicious transactions to the competent financial intelligence unit.[88] AMLD5 also introduced a definition of the term "*virtual currency*": 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.[89]

C 2018 and 2019 FATF initiatives

Since the adoption of AMLD5 in 2018, the crypto-space has not stood still. New crypto-assets were created, new types of crypto-related services emerged and new service providers entered the crypto-market. In response to these new developments, the FATF adopted

changes to its Recommendations in October 2018, to clarify that they apply to financial activities involving virtual assets, as well as related service providers.[90] It adopted two new Glossary definitions ("virtual asset" – the FATF uses the term "virtual assets" to refer to a very broad category of assets that encompasses what this chapter has called "cryptoassets" – and "virtual asset service provider"[91]) and it updated Recommendation 15.[92] In its updated form, Recommendation 15 requires countries to regulate virtual asset service providers for AML/CFT purposes, to license or register them and to subject them to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.[93] In June 2019, the FATF adopted an Interpretative Note to Recommendation 15 (INR 15) to further clarify how the FATF requirements should be applied in relation to virtual assets and virtual asset service providers. INR 15 sets out measures for effective regulation and supervision or monitoring of virtual asset service providers.[94] It requires countries to ensure that their virtual asset service providers assess and mitigate their money laundering and terrorist financing risks and implement customer due diligence controls, record-keeping, suspicious transaction reporting, and screen all transactions for compliance with targeted financial sanctions in line with other entities subject to AML/CFT regulation.[95] The FATF also adopted new Guidance on the application of the – for AML/CFT typical – risk-based approach to virtual assets and virtual asset service providers in June 2019.[96] The new Guidance expands on its 2015 Guidance for a risk-based approach to virtual currencies, which focused on the points where virtual currency activities intersect with and provide gateways to and from the traditional financial system[97] (*i.e.* so-called virtual currency to fiat currency exchanges[98]).

D Current EU AML/CFT framework already outdated and insufficient

In Table 11.1 a side-by-side comparison of the FATF standards on virtual assets with the AML/CFT-regime for virtual currencies set out in AMLD5 shows that the first EU AML/CFT-regime for virtual currencies already lags behind what is considered the current international AML/CFT-standard for cryptoassets (emphasis added in italics).

A first observation is that the AMLD5 definition of "virtual currencies" is a lot narrower than the FATF definition of "virtual assets". It only covers what this chapter has labelled "cryptocurrencies" and does not encompass other types of cryptoassets, most notably tokens.

Secondly, various cryptoasset actors targeted by the FATF Recommendations are not covered by AMLD5:[99]

- platforms that only offer crypto-to-crypto (*i.e.* virtual to virtual asset) exchange services;
- platforms that facilitate the transfer of cryptoassets as an intermediary; and
- persons that are active in the participation in and provision of financial services related to an issuer's offer and/or sale of cryptoassets.

When AMLD5 was conceived, the European legislator did not pay a lot of attention to the existence of these actors and the potential AML/CFT risks they posed. Meanwhile risk awareness has grown. Not only on the EU level, within regulatory bodies like the European Securities and Markets Authority (ESMA) and the European Banking Authority (EBA), [100] but also on the level of national Member States.[101] AMLD5 may only just be in force, from a regulatory perspective, it is already outdated and insufficient to deal with the AML/CFT risks cryptoassets pose today.

Table 11.1 Comparison of the FATF standards on virtual assets with the AML/CFT-regime for virtual currencies set-out in AMLD5

	AMLD5	*FATF Recommendations*
ASSETS	**Virtual currencies** 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.[1]	A **virtual asset** is a 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.
OBLIGED ENTITIES	**Providers engaged in exchange services between virtual currencies and fiat currencies. Custodian wallet** provider means an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies.[2]	**Virtual asset service provider** means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i) exchange between virtual assets and fiat currencies; ii) *exchange between one or more forms of virtual assets*; iii) *transfer of virtual assets*; iv) safekeeping and/or *administration of virtual assets or instruments enabling control over virtual assets*; and v) *participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset*.

Note: 1: Article 3(18) AMLD4. 2: Article 3(19) AMLD4.

E Suggestions for future regulation

To bring the European AML/CFT framework up to speed with the current reality in the crypto-space, a number of regulatory actions can be considered.

1° Broaden the definition of virtual currencies

Firstly, in light of the FATF definition of virtual assets, the scope of the definition of virtual currencies can be broadened.

a. Tokens

The definition of virtual currencies as included in the existing EU AML/CFT framework currently only covers digital representations of value that are *accepted as a means of exchange*. This is a lot narrower than the FATF definition of virtual assets cited above, as it does not

cover investment and utility tokens, [102] but only cryptocurrencies (both traditional "non-backed" cryptocurrencies and stablecoins[103]).

As the ESMA[104] and the EBA[105] have indicated in their January 2019 reports on crypto-assets (and ICOs), it would make sense to expand the scope of the definition of virtual currencies to all types of cryptoassets and to also include (investment and utility) tokens. The reason is simple: tokens make use of the same technology as cryptocurrencies. They can be transferred and stored electronically and, in many cases, traded on the exact same platforms as cryptocurrencies.[106] Their design allows them to be used as a "vehicle" to move economic value around, irrespective of their function. Therefore, they are equally suitable for money laundering and terrorist financing activities as cryptocurrencies and should be treated the same way.

b. State currencies

Moving beyond cryptocurrencies and tokens, and more controversial, it could be considered to include CBDCs[107] in the definition of virtual currencies. The concern here is that CBDCs could be used to thwart economic sanctions.[108] By including digital state currencies into the scope of the EU AML/CFT framework, and expanding the list of obliged entities, [109] the EU could ensure that questionable foreign actors who try to illegally move their wealth into or through the EU financial system using such currencies, are identified, allowing law enforcement agencies to take action against them.

c. In-game currencies

Research suggests that in-game currencies, such as "V-Bucks" used in the popular online multiplayer game Fortnite, can also be used to launder money obtained through criminal activities.[110] When in-game currencies have real life value outside of the game and can be transferred from one player to another, criminals can use them to move value around or launder illicit funds (for example cash deposited with a poorly regulated overseas bank) through them. For instance, they can buy in-game currencies with illicit funds and then sell them at a discounted rate to other players on the dark web or through social media platforms. While there is currently no hard data available to substantiate this, it is possible that criminals also make use of cryptocurrencies and/or other cryptoassets in this process to even further obfuscate transaction flows.[111]

Currently, in-game currencies are not included in AMLD5's definition of virtual currencies. It would be prudent to further study money laundering and terrorist financing through online games to obtain hard data on the actual scale of misuse. On the basis thereof, it can be assessed whether there is an actual need to include in-game currencies in the definition of virtual currencies. If there is, it would make sense to update the list of obliged entities accordingly.

2° Broaden the list of gatekeepers

Currently, as aforementioned, the EU AML/CFT framework includes only two crypto-asset gatekeepers: custodian wallet providers and providers engaged in exchange services between virtual currencies and fiat currencies. A whole variety of cryptoasset actors is not (yet) targeted. As a result, various activities can still take place outside of the scope of AMLD5. This is problematic because the blind spots can be pursued by criminals, terrorists and other illicit actors to launder money, finance terrorism and/or engage in other illicit activities, such as tax evasion.

Therefore, and in line with the FATF's definition of virtual asset service providers, more cryptoasset gatekeepers should be brought within the remit of the European AML/CFT framework. Hereinafter, we discuss the most important contenders, taking into account the aforementioned overview of key actors in cryptoasset schemes.[112]

a. Crypto-to-crypto exchanges

Crypto-to-crypto exchanges, *i.e.* the platforms that only offer exchange services from one cryptoasset to another, that are not custodian wallet providers, remain outside of AMLD5's scope. Nevertheless, they can add an extra layer of disguise to the origin of crypto-assets (when they later pass through an obliged entity) or even allow cryptoassets to be used completely outside of the monitored system.[113] That is why the FATF has included them in its latest international AML/CFT standards. To create a more adequate EU AML/CFT regime, crypto-to-crypto exchanges should also be included in the EU's list of obliged entities.

b. Cryptoasset "financial services" providers

Cryptoasset "financial services" providers, who are active in the participation in and provision of "financial services" related to an issuer's offer and/or sale of a cryptoasset, fall outside of the scope of AMLD5. As the FATF has rightly pointed out, it makes sense to also bring these actors into the scope of the EU AML/CFT framework, because they engage in similar activities as financial institutions who participate in the issuance of securities and provide financial services in relation to such issues ("same risk, same approach").[114] The EU should adhere to these FATF findings.

c. Trading platforms

Neither centrally operated trading platforms, enabling buyers and sellers of cryptoassets to find each other online, nor their decentralised counterparts, are currently obliged entities under AMLD5. Centrally operated trading platforms are, however, covered by the FATF's AML/CFT standards.[115] The EU would again do well to follow the FATF's lead, so that illegal transactions facilitated by a trading platform become visible.

Pure peer-to-peer, decentralised trading platforms are not included in the FATF's scope. This can be understood: regulating decentralised trading platforms is very hard, because there is no one to attach regulation to. Nevertheless, the money laundering and terrorist finance risks that decentralised trading platforms pose, should be further assessed and, in view of such risk assessment, adequately addressed.[116]

d. Issuers of cryptoassets

Currently, issuers of cryptoassets fall outside the scope of both the EU AML/CFT framework and the FATF standards. There is, however, a compelling argument to include issuers of cryptoassets as AML/CFT gatekeepers: they do not necessarily use traditional financial service providers, who are in scope of the EU AML/CFT framework,[117] to structure and conduct the issuance and sale of cryptoassets to prospective users. On the contrary, there are normally no intermediaries involved in the whole process and users buy their cryptoassets, usually tokens or coins that are not mined, directly from the issuer. With that in mind, and having regard of the fact that all cryptoassets possess the same risk for money laundering and terrorist financing from a technical perspective,[118] bringing issuers of cryptoassets into the scope of the AML/CFT framework makes sense.[119]

e. Non-custodian wallet providers

Non-custodian wallet providers, *i.e.* hardware and software wallet providers, are not targeted by the EU AML/CFT framework, nor by the FATF standards, Hence, users using

software or hardware wallets escape AML/CFT due diligence checks, as long as they also stay away from exchanges exchanging cryptocurrencies into fiat money.

In its June 2019 Guidance on the application of the risk-based approach to virtual assets and virtual asset service providers the FATF indicated that it does not seek to regulate persons that provide ancillary services or products to a virtual asset network, including hardware wallet manufacturers and non-custodial wallets, as virtual asset service providers.[120] We see no reason to derogate from this Guidance. Non-custodian wallet providers only provide the technical tools for others to work with and typically do not function as intermediaries, so it does not make much sense to target them for AML/CFT purposes.

f. Cryptoasset creators

Just like non-custodian wallet providers, cryptoasset creators only provide the technological tools for others to work with.[121] Therefore, and as for non-custodian wallet providers, it does not make much sense to target them for AML/CFT purposes.

g. Miners

More analysis is required for miners.

When the text of AMLD5 was drawn up, the European Commission saw two main reasons not to include miners as AML/CFT gatekeepers:

- they were considered to be more a sort of technical service provider than gatekeepers between the virtual sphere and the real world; and
- they were thought to be (big energy-consuming Bitcoin farms) mostly located in China, which would make any initiative to target them largely impossible to enforce.[122]

The second reason may have had factual grounds when the Commission started studying mining back in 2015–2016, but a lot has changed since then. Mining activity has become more geographically distributed, with China losing relative "market share" to some North American and Scandinavian regions and some Western European countries (e.g., France) also seeing a rising level of activity.[123] Moreover, the mining community of 2020 is nothing like that of 2016. First of all, a lot of miners have diversified their activities in terms of the number of coins they mine and are no longer focusing on Bitcoin alone.[124] In addition, new coins have emerged that do not always require big energy-consuming server farms to mine, but that can be mined running a few hardware rigs at home. Such rigs can be set up by anyone, including criminal actors.[125]

Regulators should be aware that by mining coins, directly or indirectly via front men, criminal actors can get access to clean cash. Newly mined coins are by definition "clean", so if someone (e.g., a bank) is willing to convert them into fiat currency or other cryptoassets, the resulting funds are also clean. This is a reality that is hard to address from a regulatory perspective. A first step could be to try to map the use of this technique and subsequently, if it effectively proves an important blind spot in the fight against money laundering and terrorist financing, to take appropriate counter measures.

3° User registration

In its 2016 Impact Assessment, drafted and published in the build-up to AMLD5,[126] the Commission put forward a number of options to address the money laundering and terrorist financing risks surrounding virtual currencies. One of the options presented

was to target the users of virtual currencies and lift their anonymity. The Commission saw two scenarios to do this: a mandatory registration of users, or a voluntary self-registration of users. Neither of these scenarios were adopted in the end. However, in the final, adopted, text of AMLD5 the Commission did commit itself to draw up a report on the implementation of the Directive by 11 January 2022, and submit it to the European Parliament and the Council. Article 1(44) of AMLD5 provides that "*the report shall be accompanied, if necessary, by appropriate legislative proposals, including, where appropriate, with respect to virtual currencies, empowerments to set-up and maintain a central database registering users' identities and wallet addresses accessible to FIUs, as well as self-declaration forms for the use of virtual currency users*" (own emphasis added). This seems to point to a system of voluntary self-registration of users.

During its last supranational risk assessment (published in July 2019), the Commission did not mention user registration anymore. This can be an indication that a system of user registration is not considered a priority and perhaps even that it is off the table. Anyway, even if a system of voluntary self-registration of users were to be put in place, it is very doubtful that the category that should be targeted the most, users of cryptoassets for illicit purposes, would voluntarily register as a user: that would be like trusting the thief to come to the police station voluntarily after committing a theft.[127]

For users who hold their virtual currencies via a custodian wallet provider or enter into virtual currency transactions via a virtual exchange platform within the meaning of AMLD5, there is of course no issue: such users can no longer be anonymous, because of the customer due diligence requirements vested upon the custodian wallet providers and virtual currency exchange platforms introduced by AMLD5.

4° An EU AML/CFT watchdog

Cryptoassets are not tied to national borders, nor are the money laundering and terrorist financing and other illicit activities for which they are sometimes used. Nevertheless, and although within the EU the AML/CFT regulatory framework is of European origin, compliance with AML/CFT laws is monitored by domestic supervisors. If supervisory authorities and law enforcement agencies want to stand a realistic chance in the fight against criminal activities via cryptoassets they need to work together and share information. In reality, this does not always happen: cross-border cooperation and coordination between national authorities in the field of AML/CFT still leave much to be desired.[128] To address this issue, on 5 December 2019 the EU Council (ECOFIN) formally invited the Commission "*to explore in particular the possibilities, advantages and disadvantages of conferring certain responsibilities and powers for AML supervision to a Union body with an independent structure and direct powers vis-à-vis certain obliged entities*".[129] We endorse this call. The introduction of a European AML/CFT watchdog could have various benefits, especially if it is staffed with highly trained IT personnel capable of analysing the AML/CFT risks new technologies bring. It could help promote information-sharing, serve as a new knowledge pool, and provide a more independent approach to AML/CFT cases.

5° A cashless society with digital money and fully traceable coins as a utopia

Thinking somewhat out of the box, replacing cash by a public, traceable CBDC, or a private equivalent thereof, could theoretically mark the end of many money laundering and other

criminal activities. If all payment information[130] is instantly available to law enforcement agencies, or can easily be made available to them, illicit actors will no longer be able to operate in the dark, effectively forcing them to cease many of their operations. However, it is unlikely that citizens will want to fully give up on cash payments any time soon, let alone agree to governments monitoring every payment they make.[131] They do not want central banks and government authorities to have insight into all details of their payment transactions. Therefore, politically, the cashless society, a "dream scenario" for supervisory authorities, is most likely a utopia.

To overcome citizen's concerns, the challenge for central banks is to design and implement a CBDC that strikes a balance between their demand for user integrity, and the need to comply with AML/CFT standards. In this respect, the so-called EUROchain research network has recently made a noteworthy effort to find such balance.[132] It has developed a proof of concept for anonymity in digital cash, more in particular a token-based variant of a CBDC with cash-like features. In short, EUROchain's proof of concept provides a digitalisation solution for AML/CFT compliance procedures whereby a user's identity and transaction history cannot be seen by the central bank or intermediaries other than those chosen by the user. The enforcement of limits on anonymous electronic transactions is automated, and additional AML/CFT checks are delegated to a dedicated AML authority, which checks the identities of users involved in large-value transactions and prevents CBDC from being transferred to embargoed users. All of this is technically achieved using "anonymity vouchers", which allow users to anonymously transfer a limited amount of CBDC over a defined period of time.

VI A brief note on cybersecurity

Cryptoassets are often stored online at online storage providers (custodian wallet providers) or crypto-exchanges which offer custody services to their customers.[133] Such online storage makes the cryptoassets susceptible to hack attacks and online theft. Stolen cryptoassets typically find their way to illegal markets and are used to fund further criminal activity.[134]

There are currently no specific EU laws that set out minimum standards for cybersecurity that intermediaries who offer custodial services for cryptoassets have to comply with. In view of the growing number of security breaches resulting in thefts of cryptoassets,[135] it is recommendable to change this.[136] A line of thought could be to require intermediaries offering custodial services to (i) draw up and implement an IT risk management policy adhering to certain IT security standards, and (ii) appoint an independent IT expert to conduct an external security audit on a regular basis.

An additional cybersecurity concern relates to so-called ransomware attacks. Criminals who are involved in such ransomware attacks, whereby the access to computers and networks is locked until the victim pays a certain ransom, often ask victims to pay the ransom in cryptocurrencies, allowing the criminals to monetise on ransomware attacks without revealing their real-life identities.[137]

To the extent technically feasible, a regulatory response to make it harder for criminals to use the crypto-ransoms they have collected for other, future, transactions could be to blacklist the coins used to pay a crypto-ransom.[138] The coins would get a "tag" so to speak, much like physical banknotes would get marked, which would make it more difficult for criminals to move them through legitimate channels or effectively spend them, making the collection of a crypto-ransom less interesting.

VII Subsidiarity: rulemaking at the right level

As aforementioned, money laundering and terrorist financing via cryptoassets is not bound by any border.[139] It is, therefore, a global issue that should be addressed globally. As an intergovernmental "policy-making body" setting AML/CFT standards at the international level, the FATF is doing precisely that. From an EU perspective, the EU and its Member States should continue to contribute to the work of the FATF and the international standards set by the FATF should continue to be incorporated into EU law to ensure full compliance throughout the internal market and the international financial system.[140]

In this respect, the EU could do better. As illustrated on p.172, the latest EU AML/CFT rules for virtual currencies, set out in AMLD5, were already outdated well before EU Member States were supposed to transpose them into their national AML/CFT laws, *i.e.* on 10 January 2020.[141] The EU is clearly lagging behind on international AML/CFT standards and has regulatory work to do.

If the EU remains inactive, individual Member States could already take the lead – and perhaps even should, given the risk-based approach of the EU AML/CFT framework and their individual memberships of the FATF – and amend their domestic AML/CFT legislation to comply with the latest FATF Recommendations, or even go beyond.[142] It is, however, clear that such domestic actions alone are not sufficient: to avoid an unlevel playing field, regulatory arbitrage and legal uncertainty in a cross-border context, in the EU, rulemaking on cryptoassets should take place at the EU level, in the execution of international standards. To the extent that the international framework and, in the execution thereof, the EU AML/CFT framework would still leave important blind spots in the fight against money laundering and terrorist financing, Member States should consider implementing additional protection[143] (but not lesser protection), insofar as such additional protection can be justified after careful consideration of all the relevant interests, especially effective law enforcement versus data privacy interests.[144]

VIII Conclusion

At the start of 2020, over 5,100 cryptoassets existed with a total market capitalisation exceeding $250 billion. Cryptoassets can be used both for legal and illegal purposes. The use of cryptoassets for illegal purposes is not a marginal phenomenon. Illustrative is that almost half of all (yearly) transactions in Bitcoin can be linked to illegal activity, amounting to approximately $76 billion of illegal activity per year involving Bitcoin; a number that comes very close to the US and EU markets for illegal drugs. As the crypto-market is still dominated by Bitcoin, with a dominance in terms of total market capitalisation exceeding 63% ($159 billion), this is an important observation.

The key issue that needs to be addressed in order to adequately capture cryptoassets and cryptoasset actors in legislation is to unveil the anonymity, varying from pseudo-anonymity to complete anonymity, which surrounds them. This anonymity prevents cryptoasset transactions from being adequately monitored, allowing shady transactions to occur outside of the regulatory perimeter and allowing criminal organisations to use cryptoassets to obtain easy access to "clean cash" (both cash in and cash out). Additional complicating factors for adequate regulation are the intrinsically cross-border nature of cryptoassets, crypto-markets and crypto-actors and the fact that sometimes there is no central intermediary, such as an issuer, that would normally be the focal point of regulation.

The existing EU regulatory framework deals poorly with these issues. Up until the fifth revision, the EU AML/CFT framework (AMLD5), which was adopted in 2018 and became fully operational on 10 January 2020, did not include any cryptoasset gatekeeper, *de facto* exempting crypto-activity completely from the scope of EU AML/CFT legislation. Only as of said fifth revision, the EU framework includes a definition of virtual currencies and labels custodian wallet providers and virtual currency exchanges as obliged entities, requiring them to comply with the same AML/CFT requirements as banks and other financial institutions, including performing customer due diligence checks and reporting suspicious transactions to the competent financial intelligence unit.

Since the adoption of AMLD5 in 2018, the crypto-space has not stood still. New cryptoassets were created, new types of crypto-related services emerged and new service providers entered the crypto-market. In response to these new developments, the FATF took a further stance on cryptoassets in various policy documents in 2018 and 2019. A comparison of the latest FATF standards on virtual assets with the AML/CFT-regime for virtual currencies set out in AMLD5 shows that the first EU AML/CFT-regime for virtual currencies already lags behind what is considered the current international AML/CFT-standard for cryptoassets.

To bring the EU AML/CFT framework up to speed with the current reality in the crypto-space, a number of regulatory actions can be considered, including broadening the definition of virtual currencies, adding additional cryptoasset gatekeepers to the list of obliged entities and introducing an EU AML/CFT watchdog. In addition, some measures to enhance cybersecurity can be given consideration, under which the further exploration of the possibilities of coin blacklisting.

Money laundering and terrorist financing via cryptoassets is not bound by any border. It is, therefore, a global issue that should be addressed globally. As an intergovernmental "policy-making body" setting AML/CFT standards at the international level, the FATF is doing precisely that. From an EU perspective, the EU and its Member States should continue to contribute to the work of the FATF and the international standards set by the FATF should continue to be incorporated into EU law to ensure full compliance throughout the internal market and the international financial system. In this respect, the EU can do a better job than it is doing now.

Notes

1 Statement made on the basis of data derived from https://coinmarketcap.com on 4 March 2020.
2 S. FOLEY, J. R. KARLSEN and T. J. PUTNIŅŠ, "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?", December 2018, 27 (electronically available via https://ssrn.com/abstract=3102645). See for a similar observation: G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 1.
3 S. FOLEY, J. R. KARLSEN and T. J. PUTNIŅŠ, "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?", December 2018, 26 (electronically available via https://ssrn.com/abstract=3102645).
4 Data derived from https://coinmarketcap.com on 4 March 2020.
5 R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, 45 and 48 (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).
6 Data derived from https://coinmarketcap.com on 4 March 2020.

7 CIPHERTRACE CRYPTOCURRENCY INTELLIGENCE, "Cryptocurrency anti-money laundering report, 2019 Q3", November 2019, 34 (electronically available via https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/).

8 See for a number of examples on non-EU measures on cryptocurrencies: T. KEATINGE, D. CARLISLE and F. KEEN, "Virtual currencies and terrorist financing: assessing the risks and evaluating responses", study commissioned by the Directorate General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs, May 2018, 47–50 (electronically available via http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf). See also: P. VALENTE, "Bitcoin and virtual currencies are real: are regulators still virtual?", INTERTAX, Volume 46, Issue 6 & 7, 546–547.

9 See e.g. E. HERLIN-KARNELL and N. RYDER, "The robustness of EU financial crimes legislation: a critical review of the EU and UK anti-fraud and money laundering scheme", 2017, *European Business Law Review*, No. 4, 1–39.

10 Also see below, section V, subsection B.

11 It is often technologically feasible to link cryptocurrency transactions to real-life identities if great effort is made, making cryptocurrencies pseudonymous. However, certain services like mixers and tumblers allow for reduced transparency and increased obfuscation of financial flows, allowing for a high degree of anonymity. See also FATF, "Guidance for a risk-based approach to virtual assets and virtual asset service providers", June 2019, www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html, 6 and 36.

12 See e.g., S. ROYER, "Bitcoins in het Belgische strafrecht en strafprocesrecht", RW 2016–17, No. 13, 486; R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, 100p. (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf); EUROPEAN COMMISSION, "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, 100; L. HAFFKE, M. FROMBERGE and P. ZIMMERMANN, "Virtual currencies and anti-money laundering – the shortcomings of the 5th AML Directive (EU) and how to address them", February 2019, 1 (electronically available via https://ssrn.com/abstract=3328064)

13 M. RAUCHS, A. BLANDIN, K. KLEIN, G. PIETERS, M. RECANATINI and B. ZHANG, "2nd Global Cryptoasset Benchmarking Study", December 2018, 17 (electronically available via https://ssrn.com/abstract=3306125). It should be noted that, even though the use of the term "crypto-assets" is becoming more and more widespread, there are still various legal texts and policy documents that use different terms, such as virtual currencies, coins, digital currencies or digital assets to refer to some or all types of crypto-assets. If and when necessary, this chapter will further frame these terms within a broader taxonomy of crypto-assets.

14 However, in the EU this could change in the near future, as the European Commission has proposed the introduction of a Regulation on Markets in Crypto-assets (MiCA). The MiCA proposal includes the following definition of a crypto-asset: "*a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology*" (art. 3.1.(2)). See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593.

15 The European Central Bank (ECB) Crypto-Assets Task Force has defined the term very narrowly as *"any asset recorded in digital form that is not and does not represent either a financial claim on, or a financial liability of, any natural or legal person, and which does not embody a proprietary right against an entity"*(ECB CRYPTO-ASSETS TASK FORCE, "Crypto-assets: implications for financial stability, monetary policy, and payments and market infrastructures", *ECB Occasional Paper No. 223*, May 2019, 7 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf)). The International Organization of Securities Commissions (IOSCO) has defined the term as *"a type of private asset that depends primarily on cryptography and DLT or similar technology as part of its perceived or inherent value, and can represent an asset such as a currency, commodity or security, or be a derivative on a commodity or security"* (IOSCO, "Consultation

Report on the issues, risks and regulatory considerations relating to crypto-asset trading platforms", May 2019, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD627.pdf, 1; IOSCO, "Final Report on the issues, risks and regulatory considerations relating to crypto-asset trading platforms", February 2020, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf, 1). The Financial Stability Board (FSB) has put forward a similar definition and defines the term as "a type of private asset that depends primarily on cryptography and distributed ledger or similar technology as part of their perceived or inherent value". This definition is also referred to in the Bank of International Settlements (BIS) documentation (G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 1). In line with the FSB's definition, the European Securities and Markets Authority (ESMA) has defined a crypto-asset as *"a type of private asset that depends primarily on cryptography and DLT or similar technology as part of their perceived or inherent value"*. ESMA uses the term to refer both to so-called 'virtual currencies' and 'digital tokens' (which it defines as *"any digital representation of an interest, which may be of value, a right to receive a benefit or perform specified functions or may not have a specified purpose or use"*). According to the ESMA, crypto-asset additionally means an asset that is not issued by a central bank (ESMA, "Advice on initial coins offerings and crypto-assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, 42).

16 The EBA has defined a crypto-asset as *"an asset that: a) depends primarily on cryptography and DLT or similar technology as part of its perceived or inherent value, b) is neither issued nor guaranteed by a central bank or public authority, and c) can be used as a means of exchange and/or for investment purposes and/or to access a good or service"* (EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 10–11).

17 A reference to the perceived or inherent value of the asset having to stem at least in part from the use of cryptography and DLT or similar technology (as contained in the EBA's definition), has been left out of this working definition. This has been done to ensure that it includes all types of "stablecoins" (see further p.166–167), the perceived or inherent value of which does not necessarily stem from the use of cryptography and DLT, but rather from their redeemability and backing. The working definition put forward in this study is, admittedly, very broad, but in line with recent scholarly debate (see *inter alia* A. SNYERS and K. PAUWELS, "De ITO: a new kid on the block in het kapitaalmarktenrecht", TBH 2019/2, (174) 179–181; C. BROWN, T. DOLAN and K. BUTLER, "Crypto-assets and initial coin offerings" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (74) 75; S. BLEMUS and D. GUEGAN, "Initial crypto-asset offerings (ICOs), tokenization and corporate governance", January 2019, 7 (electronically available via https://ssrn.com/abstract=3350771); F. ANNUNZIATA, "Speak, if you can: What are you? An alternative approach to the qualification of tokens and initial coin offerings", Bocconi Legal Studies Research Paper No. 2636561, February 2019, 3–7 (electronically available via https://ssrn.com/abstract=3332485); L. PERLMAN, "A model crypto-asset regulatory framework", May 2019, 1 (electronically available via https://ssrn.com/abstract=3370679); M. NANNINGS, "Kwalificatie van crypto-assets als effect", TFR 2019/12, (623) 623–625) and instrumental to the scope of the research.

18 A. SNYERS and K. PAUWELS, "ICOs in Belgium: down the rabbit hole into legal no man's land? Part 1", *ICCLR* 2018, Vol. 29, Issue 8, (483) 485–487; F. ANNUNZIATA, "Speak, if you can: What are you? An alternative approach to the qualification of tokens and initial coin offerings", Bocconi Legal Studies Research Paper No. 2636561, February 2019, 21–24 (electronically available via https://ssrn.com/abstract=3332485).

19 C. BROWN, T. DOLAN and K. BUTLER, "Crypto-assets and initial coin offerings", in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (74) 76.

20 Also see the analysis set out in R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, 20–23 (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).

21 A. SNYERS and K. PAUWELS, "De ITO: a new kid on the block in het kapitaalmarktenrecht", TBH 2019/2, (174) 179–181; T. MAAS, "Initial coin offerings: when are tokens

securities in the EU and US?", February 2019, 21–23 (electronically available via https://ssrn.com/abstract=3337514); M. NANNINGS, "Kwalificatie van crypto-assets als effect", TFR 2019/12, (623) 624–625.

22 ESMA, "Advice on initial coins offerings and crypto-assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, 42; C. BROWN, T. DOLAN and K. BUTLER, "Crypto-assets and initial coin offerings" in J. MADIR (ed.), Fintech – Law and Regulation, Cheltenham, Edward Elgar Publishing, 2019, (74) 76.

23 F. ANNUNZIATA, "Speak, if you can: What are you? An alternative approach to the qualification of tokens and initial coin offerings", Bocconi Legal Studies Research Paper No. 2636561, February 2019, 4 (electronically available via https://ssrn.com/abstract=3332485).

24 See https://bitcoin.org/bitcoin.pdf. For a brief historical overview, also see: T. MAAS, "Initial coin offerings: when are tokens securities in the EU and US?", February 2019, 15–17 (electronically available via https://ssrn.com/abstract=3337514).

25 F. ANNUNZIATA, "Speak, if you can: What are you? An alternative approach to the qualification of tokens and initial coin offerings", Bocconi Legal Studies Research Paper No. 2636561, February 2019, 4 (electronically available via https://ssrn.com/abstract=3332485).

26 See *inter alia* EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 7; ESMA, "Advice on initial coins offerings and crypto-assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, 19; A. SNYERS and K. PAUWELS, "ICOs in Belgium: down the rabbit hole into legal no man's land? Part 1", ICCLR 2018, Vol. 29, Issue 8, (483) 489–491; C. BROWN, T. DOLAN and K. BUTLER, "Crypto-assets and initial coin offerings" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (74) 76–77; M. NANNINGS, "Kwalificatie van crypto-assets als effect", TFR 2019/12, (623) 623–624.

27 EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 7.

28 See below, subsection E.

29 S. BLEMUS and D. GUEGAN, "Initial crypto-asset offerings (ICOs), tokenization and corporate governance", January 2019, 8 (electronically available via https://ssrn.com/abstract=3350771).

30 A. SNYERS and K. PAUWELS, "De ITO: a new kid on the block in het kapitaalmarktenrecht", TBH 2019/2, (174) 182, footnote 103; M. NANNINGS, "Kwalificatie van crypto-assets als effect", TFR 2019/12, (623) 624.

31 S. BLEMUS and D. GUEGAN, "Initial Crypto-Asset Offerings (ICOs), Tokenization and Corporate Governance", January 2019, 9 (electronically available via https://ssrn.com/abstract=3350771).

32 EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 7.

33 A. SNYERS and K. PAUWELS, "ICOs in Belgium: down the rabbit hole into legal no man's land? Part 1", ICCLR 2018, Vol. 29, Issue 8, (483) 491

34 C. BROWN, T. DOLAN and K. BUTLER, "Crypto-Assets and Initial Coin Offerings" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (74) 77.

35 T. MAAS, "Initial coin offerings: when are tokens securities in the EU and US?", February 2019, 27 and 29 (electronically available via https://ssrn.com/abstract=3337514).

36 F. ANNUNZIATA, "Speak, if you can: What are you? An alternative approach to the qualification of tokens and initial coin offerings", Bocconi Legal Studies Research Paper No. 2636561, February 2019, 21 and 25 (electronically available via https://ssrn.com/abstract=3332485); M. NANNINGS, "Kwalificatie van crypto-assets als effect", TFR 2019/12, (623) 624.

37 OMFIF and IBM, "Retail CBDCs. The next payments frontier", 2019, 35 (electronically available via https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf); U. BINDSEIL, "Central bank digital currency: financial system implications and control", July 2019, 2 (electronically available via https://ssrn.com/abstract=3385283).

38 C. BARONTINI and H. HOLDEN, "Proceeding with caution – a survey on central bank digital currency" (BIS Papers No 101), January 2019, https://www.bis.org/publ/bppdf/bispap101.pdf, 11.

39 The text reflects the status as at March 2020. Events that occurred after, such as the release of the Eurosystem report on a digital euro and the subsequent ECB public consultation on the digital euro, could no longer be taken into account.

40 OMFIF and IBM, "Retail CBDCs. The next payments frontier", 2019, 2 and 9 (electronically available via https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf).
41 Various central banking and monetary policy institutions have stressed that issuing a CBDC is not contingent upon the use of a specific technology such as DLT. See C. BARONTINI and H. HOLDEN, "Proceeding with caution – a survey on central bank digital currency" (BIS Papers No 101), January 2019, https://www.bis.org/publ/bppdf/bispap101.pdf, 3; ECB CRYPTO-ASSETS TASK FORCE, "Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures", ECB Occasional Paper No. 223, May 2019, 32 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf); OMFIF and IBM, "Retail CBDCs. The next payments frontier", 2019, 35 (electronically available via https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf).
42 D. A. ZETZSCHE, R. P. BUCKLEY and D. W. ARNER, "Regulating LIBRA: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses", European Banking Institute Working Paper Series 2019/44, July 2019, 3 (electronically available via https://ssrn.com/abstract=3414401).
43 ECB CRYPTO-ASSETS TASK FORCE, "Crypto-assets: implications for financial stability, monetary policy, and payments and market infrastructures", ECB Occasional Paper No. 223, May 2019, 8 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf).
44 D. BULLMANN, J. KLEMM and A. PINNA, "In search for stability in crypto-assets: are stablecoins the solution?", ECB Occasional Paper No. 230, August 2019, 6 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf).
45 H. DE VAUPLANE, "Cryptocurrencies and Central Banks" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (102) 113.
46 *Cf.* OMFIF and IBM, "Retail CBDCs. The next payments frontier", 2019, 9 (electronically available via https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf).
47 D. BULLMANN, J. KLEMM and A. PINNA, "In search for stability in crypto-assets: are stablecoins the solution?", ECB Occasional Paper No. 230, August 2019, 6 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf); G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 1.
48 OMFIF and IBM, "Retail CBDCs. The next payments frontier", 2019, 2 (electronically available via https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf). See also V. BRÜL, "Libra – a differentiated view on Facebook's virtual currency project", *Intereconomics* 2020/1 (ZBW – Leibniz Information Centre for Economics), 55.
49 See also D. A. ZETZSCHE, R. P. BUCKLEY and D. W. ARNER, "Regulating LIBRA: the transformative potential of Facebook's cryptocurrency and possible regulatory responses", European Banking Institute Working Paper Series 2019/44, July 2019, 6 (electronically available via https://ssrn.com/abstract=3414401).
50 G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 1.
51 For example, the popular website https://coinmarketcap.com lists stablecoins such as Tether and DAI as tokens.
52 EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 7.
53 G7 WORKING GROUP ON STABLECOINS, "Investigating the impact of global stablecoins", October 2019, https://www.bis.org/cpmi/publ/d187.pdf, 2.
54 FSB, "Regulatory issues of stablecoins", October 2019, https://www.fsb.org/wp-content/uploads/P181019.pdf, 1; G20, "Press release on global stablecoins", October 2019, https://www.boj.or.jp/en/announcements/release_2019/data/rel191021e1.pdf, 1; IOSCO, "Statement on IOSCO study of emerging global stablecoin proposals", November 2019, https://www.iosco.org/news/pdf/IOSCONEWS550.pdf, 1.
55 See also: C. BROWN, T. DOLAN and K. BUTLER, "Crypto-assets and initial coin offerings" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (74) 77.

56 T. MAAS, "Initial coin offerings: when are tokens securities in the EU and US?", February 2019, 9 (electronically available via https://ssrn.com/abstract=3337514).
57 See *inter alia* ESMA, "Advice on initial coins offerings and crypto-assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, 11; EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets,
58 C. LE MOIGN, "ICO françaises: un nouveau mode de financement?", November 2018, 5 (electronically available via https://www.amf-france.org/Publications/Lettres-et-cahiers/Risques-et-tendances/Archives?docId=workspace%3A%2F%2FSpacesStore%2F27604d2f-6f2b-4877-98d4-6b1cf0a1914b).
59 C. BROWN, T. DOLAN and K. BUTLER, "Crypto-assets and initial coin offerings" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (74) 77.
60 T. MAAS, "Initial coin offerings: when are tokens securities in the EU and US?", February 2019, 15 (electronically available via https://ssrn.com/abstract=3337514).
61 C. BROWN, T. DOLAN and K. BUTLER, "Crypto-assets and initial coin offerings" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (74) 77.
62 Also see S. BLEMUS and D. GUEGAN, "Initial crypto-asset offerings (ICOs), tokenization and corporate governance", January 2019, 7 (electronically available via https://ssrn.com/abstract=3350771).
63 See e.g., ECB, "Virtual currency schemes – a further analysis", February 2015, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, 7; FATF, "Virtual currencies – key definitions and potential AML/CFT risks", June 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, 7.
64 Miners are only relevant actors for crypto-assets that can be mined, basically cryptocurrencies that are issued on a permissionless platform. On this, see: R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).
65 See e.g. FATF, "Virtual currencies – key definitions and potential AML/CFT risks", June 2014, http://www.fatf gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, 7.
66 See e.g. ECB, "Virtual currency schemes – a further analysis", February 2015, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, 8; A. MARSHALL, "P2P cryptocurrency exchanges, explained", April 2017, https://cointelegraph.com/explained/p2p-cryptocurrency-exchanges-explained.
67 See e.g. FATF, "Virtual currencies – key definitions and potential AML/CFT risks", June 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, 8; ECB, "Virtual currency schemes – a further analysis", February 2015, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, 8; KEATINGE, D. CARLISLE and F. KEEN, "Virtual currencies and terrorist financing: assessing the risks and evaluating responses", study commissioned by the Directorate General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs, May 2018, 14 (electronically available via http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf).
68 See above, section II, subsection E and below, section IV.
69 Between brackets because we are not referring to the regulated term financial services, which is used as a connecting factor for traditional financial services regulation.
70 See: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/encryption_en. We raise the issue, but will not elaborate on data protection and privacy aspects further. On the interaction between blockchain and the GDPR, see e.g., M. FINCK, "Blockchains and data protection in the European Union", Max Planck Institute for Innovation & Competition Research Paper No. 18-01, 30 November 2017, 32p. (electronically available via https://ssrn.com/abstract=3080322).
71 IMF Staff Discussion Note, "Virtual currencies and beyond: initial considerations", January 2016, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf, 25 and 27.

72 ECB, "Virtual currency schemes – a further analysis", February 2015, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, 28.
73 See section VII.
74 IMF Staff Discussion Note, "Virtual currencies and beyond: initial considerations", January 2016, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf, 25.
75 Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering, OJ L 166, 28 June 1991, 77 (electronically available via https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31991L0308&from=EN).
76 Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering, OJ L 344, 28 December 2001, 76, (electronically available via https://eur-lex.europa.eu/resource.html?uri=cellar:57ce32a4-2d5b-48f6-adb0-c1c4c7f7a192.0004.02/DOC_1&format=PDF).
77 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25 November 2005, 15 (electronically available via https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0060&from=EN), accompanied by Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community, OJ L 309, 25 November 2005, 9 (electronically available via: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005R1889&from=EN).
78 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141, 5 June 2015, 73 (electronically available via https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=En), accompanied by the EU Funds Transfer Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, OJ L 141, 5 June 2015, 1 (electronically available via https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R0847).
79 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, OJ L 156, 19 June 2018, 43–74.
80 E.g. I. BANTEKAS and S. NASH, *International Criminal Law*, Routledge-Cavendish, 2007, 247; S. ROYER, "Bitcoins in het Belgische strafrecht en strafprocesrecht", RW 2016–17, No. 13, 491; E. HERLIN-KARNELL and N. RYDER, "The robustness of EU financial crimes legislation: a critical review of the EU and UK Anti-Fraud and Money Laundering Scheme", *European Business Law Review*, 2017, No. 4, 1–39.
81 E.g. N. VANDEZANDE, Virtual currencies: a legal framework, Antwerp, Intersentia, 2018, 278.
82 See: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/money-laundering_en.
83 Article 2, 1 AMLD4.
84 Because traditional gatekeepers were, as a rule, not involved in crypto-activity.
85 Article 4 AMLD5.
86 See e.g. Commission Staff Working Document Impact Assessment Accompanying the document "Proposal for a Directive of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC", SWD/2016/0223 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0223&from=EN.
87 Article 3(19) AMLD4, as added by Article 1 of AMLD5.
88 EUROPEAN SUPERVISORY AUTHORITIES (ESAs), "Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector", October 2019, https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/1605240c-57b0-49e1-bccf-60916e28b633/Joint%20

Opinion%20on%20the%20risks%20on%20ML%20and%20TF%20affecting%20the%20EU%27s%20financial%20sector.pdf?retry=1, 14; EUROPEAN COMMISSION, "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, 103.

89 Article 3(18) AMLD4, added by Article 1 of AMLD5.

90 FATF, "FATF Report to G20 Leaders' Summit", June 2019, https://www.fatf-gafi.org/media/fatf/content/images/G20-June-2019.pdf, 2.

91 See below, section V, subsection D.

92 FATF, "Guidance for a risk-based approach to virtual assets and virtual asset service providers", June 2019, www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html, 6. Also see FATF, "International standards on combating money laundering and the financing of terrorism & proliferation – the FATF Recommendations", June 2019, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf, 15 and 126–127.

93 FATF, "FATF Report to G20 Leaders' Summit", June 2019, https://www.fatf-gafi.org/media/fatf/content/images/G20-June-2019.pdf, 2; EUROPEAN COMMISSION, "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, 97.

94 FATF, "FATF Report to G20 Leaders' Summit", June 2019, https://www.fatf-gafi.org/media/fatf/content/images/G20-June-2019.pdf, 2.

95 FATF, "International standards on combating money laundering and the financing of terrorism & proliferation – the FATF Recommendations", June 2019, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf, 70–71.

96 See FATF, "Guidance for a risk-based approach to virtual assets and virtual asset service providers", June 2019, www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html, 57p.

97 FATF, "Guidance for a risk-based approach to virtual currencies", June 2015, https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf, 46p.

98 See FATF, "Guidance for a risk-based approach to virtual assets and virtual asset service providers", June 2019, www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html, 6.

99 EUROPEAN COMMISSION, "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, 103. Also see already in 2018: R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, 76–80 (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).

100 ESMA, "Advice on initial coins offerings and crypto-assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, 36; EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 20–21.

101 As highlighted in EUROPEAN COMMISSION, "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, 101–102.

102 See L. HAFFKE, M. FROMBERGE and P. ZIMMERMANN, "Virtual currencies and anti-money laundering – the shortcomings of the 5th AML Directive (EU) and how to address them", February 2019, 13 (electronically available via https://ssrn.com/abstract=3328064).

103 Insofar as they do not qualify as e-money schemes. Also see L. HAFFKE, M. FROMBERGE and P. ZIMMERMANN, "Virtual currencies and anti-money laundering – the shortcomings of the 5th AML Directive (EU) and how to address them", February 2019, 10 (electronically available via https://ssrn.com/abstract=3328064).

104 ESMA, "Advice on initial coins offerings and crypto-assets", January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, 36.

105 EBA, "Report with advice for the European Commission on crypto-assets", January 2019, https://eba.europa.eu/eba-reports-on-crypto-assets, 20–21. See also ESAs, "Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector", October 2019, https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/1605240c-57b0-49e1-bccf-60916e28b633/Joint%20Opinion%20on%20the%20risks%20on%20ML%20and%20TF%20affecting%20the%20EU%27s%20financial%20sector.pdf?retry=1, 15.

106 L. HAFFKE, M. FROMBERGE and P. ZIMMERMANN, "Virtual currencies and anti-money laundering – the shortcomings of the 5th AML Directive (EU) and how to address them", February 2019, 13 (electronically available via https://ssrn.com/abstract=3328064).

107 See section II, subsection C.

108 *Cf.* CIPHERTRACE CRYPTOCURRENCY INTELLIGENCE, "Cryptocurrency Anti-Money Laundering Report, 2019 Q3", November 2019, 29 (electronically available via https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/), on Venezuela's plans to start using crypto.

109 See section V, subsection E, *2° Broaden the list of gatekeepers*.

110 See A. MOISEIENKO and K. IZENMAN, "Gaming the system: money laundering through online games", RUSI Newsbrief Vol. 39, No. 9, October 2019, 5p. (electronically available via https://rusi.org/sites/default/files/20191011_newsbrief_vol39_no9_moiseienko_and_izenman_web.pdf).

111 *Cf.* FATF, "Guidance for a risk-based approach to virtual assets and virtual asset service providers", June 2019, www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html, 18.

112 See section III.

113 R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, 77 (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf). *Cf.* See also S. J. HUGHES, "'Gatekeepers' are vital participants in anti-money- laundering laws and enforcement regimes as permission-less Blockchain-based transactions pose challenges to current means to 'follow the money'", Indiana Legal Studies Research Paper No. 408 (2019), August 2019, 12 (electronically available via https://ssrn.com/abstract=3436098).

114 See FATF, "Guidance for a risk-based approach to virtual assets and virtual asset service providers", June 2019, www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html, 16, fn. 9.

115 See the two FATF statements on the AML/CFT treatment of trading platforms in its June 2019 Guidance, which can be summarised as follows:
- when a trading platform only provides a forum where buyers and sellers of virtual assets can post their bids and offers, and the parties themselves trade at an outside venue (either through individual wallets or other wallets not hosted by the trading platform), then that trading platform likely falls outside the FATF definition of virtual asset service provider;
- when a trading platform facilitates the exchange and/or transfer of virtual assets, or another financial activity involving virtual assets, including by purchasing virtual assets from a seller (when transactions or bids and offers are matched on the trading platform) and selling them to a buyer, then that trading platform qualifies as a virtual asset service provider conducting exchange and/or transfer activity as a business on behalf of its customers.

116 Also see section IV.

117 See section IV.
118 Also see L. HAFFKE, M. FROMBERGE and P. ZIMMERMANN, "Virtual currencies and anti-money laundering – the shortcomings of the 5th AML Directive (EU) and how to address them", February 2019, 20 (electronically available via https://ssrn.com/abstract=3328064).
119 Also see EUROPEAN COMMISSION, "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, 103.
120 See FATF, "Guidance for a risk-based approach to virtual assets and virtual asset service providers", June 2019, www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html, 17.
121 Unless of course the coin inventor would also be the coin issuer. See R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, 78 (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).
122 *Ibidem*, 76.
123 M. RAUCHS, A. BLANDIN, K. KLEIN, G. PIETERS, M. RECANATINI and B. ZHANG, "2nd Global Cryptoasset Benchmarking Study", December 2018, 80 (electronically available via https://ssrn.com/abstract=3306125).
124 *Ibidem*, 68–69.
125 R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, 76–77 (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).
126 See EUROPEAN COMMISSION, "Commission Staff Working Document Impact Assessment accompanying the document "Proposal for a Directive of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC", SWD/2016/0223 final, July 2016, https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52016SC0223, 174p.
127 R. HOUBEN and A. SNYERS, "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion", European Parliament study, July 2018, 80 (electronically available via https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).
128 See EUROPEAN COMMISSION, "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", COM(2019) 370 final, July 2019, https://op.europa.eu/en/publication-detail/-/publication/0b2ecb04-aef4-11e9-9d01-01aa75ed71a1/language-en, 20p.
129 COUNCIL OF THE EUROPEAN UNION, "Council Conclusions on strategic priorities on anti-money laundering and countering the financing of terrorism", 14823/19, December 2019, http://data.consilium.europa.eu/doc/document/ST-14823-2019-INIT/en/pdf, 7.
130 I.e. all information on the use of payment instruments and the identity of their holders.
131 Cf. H. DE VAUPLANE, "Cryptocurrencies and Central Banks" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (102) 119.
132 ECB, "Exploring anonymity in central bank digital currencies", In *Focus Issue* No 4, December 2019, 11p. (electronically available via https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf).
133 M. RAUCHS, A. BLANDIN, K. KLEIN, G. PIETERS, M. RECANATINI and B. ZHANG, "2nd Global Cryptoasset Benchmarking Study", December 2018, 63 (electronically available via https://ssrn.com/abstract=3306125). Also see IOSCO, "Consultation Report on the issues, risks and regulatory considerations relating to crypto-asset trading platforms", May 2019, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD627.pdf, 12–13; IOSCO, "Final Report on the issues, risks and regulatory considerations relating to crypto-asset trading platforms", February 2020, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf, 12–13.

134 For example, recent research by UN experts has revealed that cyber actors employed by the Democratic People's Republic of Korea have stolen an estimated $2 billion in fiat currencies and crypto-currencies from banks and crypto-exchanges to fund the production of weapons of mass destruction: M. NICHOLS, "North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report", August 2019, https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX; CIPHERTRACE CRYPTOCURRENCY INTELLIGENCE, "Cryptocurrency Anti-Money Laundering Report, 2019 Q3", November 2019, 30 (electronically available via https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/).

135 Over the past few years, users of crypto-assets have lost several hundreds of millions of US dollars' worth of crypto-asset funds as a result of security breaches at exchanges and storage facilities. In 2019, thefts were reported to even exceed a value of more than $1 billion. See: CIPHERTRACE CRYPTOCURRENCY INTELLIGENCE, "Cryptocurrency Anti-Money Laundering Report, 2019 Q3", November 2019, 17 (electronically available via https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/).

136 Also see IOSCO, "Consultation Report on the issues, risks and regulatory considerations relating to crypto-asset trading platforms", May 2019, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD627.pdf, 22–24; IOSCO, "Final Report on the issues, risks and regulatory considerations relating to crypto-asset trading platforms", February 2020, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf, 22–24.

137 CIPHERTRACE CRYPTOCURRENCY INTELLIGENCE, "Cryptocurrency Anti-Money Laundering Report, 2019 Q3", November 2019, 20–21 (electronically available via https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/); S. J. HUGHES, "'Gatekeepers' are vital participants in anti-money- laundering laws and enforcement regimes as permission-less Blockchain-based transactions pose challenges to current means to 'follow the money'", Indiana Legal Studies Research Paper No. 408 (2019), August 2019, 38 (electronically available via https://ssrn.com/abstract=3436098); X. LI and A. B. WHINSTON, "Analyzing cryptocurrencies", October 2019, 1 and 4 (electronically available via https://ssrn.com/abstract=3500276); M. MÖSER and A. NARAYANAN, "Effective cryptocurrency regulation through blacklisting", October 2019, 1 (electronically available via https://maltemoeser.de/paper/blacklisting-regulation.pdf).

138 See on the concept of blacklisting: M. MÖSER and A. NARAYANAN, "Effective cryptocurrency regulation through blacklisting", October 2019, 24p. (electronically available via https://maltemoeser.de/paper/blacklisting-regulation.pdf).

139 See section IV.

140 Also see C. BROWN, T. DOLAN and K. BUTLER, "Crypto-assets and initial coin offerings" in J. MADIR (ed.), *Fintech – Law and Regulation*, Cheltenham, Edward Elgar Publishing, 2019, (74) 79.

141 See section V, subsection B.

142 See above the blind spots not targeted by the FATF: section V, subsection E, *2° Broaden the list of gatekeepers*.

143 *Ibidem*.

144 Also see section IV.