BRIEFING
Requested by the ECON committee
Study in Focus

European Parliament

Crypto-assets

Key developments, regulatory concerns and responses

The original study[1] sets out recent developments regarding crypto-assets. These relate mainly to the continuing use of crypto-assets for money laundering and terrorist financing (ML/TF), the massive growth of private "tokens" used to raise funds, and to the emergence of stablecoins and central bank digital currencies. The study, furthermore, addresses key regulatory concerns, taking into account these recent developments, and suggests regulatory responses.

Check out the original full study by scanning this QR code!

Background

Crypto-assets are a global phenomenon: they are created by private actors in various countries all over the world, they are cross-border in their application and infrastructure, and they are easily accessible, transferable, exchangeable and tradable from nearly anywhere in the world. To address the challenges, regulatory authorities will have to step in. In some countries legislators have already taken action or are planning to do so. These national initiatives are not necessarily aligned with each other, leading to regulatory arbitrage. To avoid regulatory arbitrage, rulemaking on crypto-assets should ideally take place at the European level, preferably in the execution of international standards. At the start of 2020, over 5 100 crypto-assets exist with a total market capitalisation exceeding EUR2200 billion. Both lawful and unlawful crypto-markets exist. Most legal activity in crypto-assets – and in particular in **cryptocurrencies** – takes place on crypto-exchanges. It relates mostly to the use of cryptocurrencies for speculative purposes. The illegal activity includes, amongst others, the buying and selling of illegal goods or services online in darknet marketplaces, money laundering, evasion of capital controls, payments in ransomware attacks, and thefts. In this context, cryptocurrencies function mostly as a payment instrument. Remarkable is that almost half of all (yearly) transactions in **Bitcoin** can be linked to illegal activity. As the crypto-market is still dominated by Bitcoin, with a dominance in terms of total market capitalisation exceeding 63% (EUR140 billion), this is an important observation. As such, the use of cryptocurrencies for criminal purposes is not new and was already covered by our 2018 study *Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion*[2]. Since then, there are, however, interesting developments as regards blind spots in the fight against **financial crime** and how to address the illegal use of crypto-assets via regulation. This study addresses these new developments. In addition, and outside of the context of the use of crypto-assets in an illegal context, two notable developments since the above previous study 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).

Policy Department for Economic, Scientific and Quality of Life Policies
Directorate-General for Internal Policies
Authors: Prof. Dr. Robby HOUBEN and Alexander SNYERS
PE 648.793 - May 2020

EN

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 of "crypto-assets".

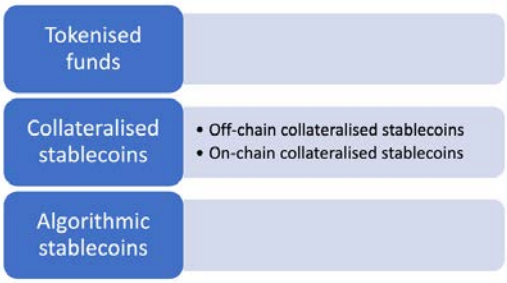
Key findings

This study focusses on crypto-assets in this broader sense, and hence, also scrutinizes tokens, stablecoins and CBDCs. As regards CBDCs, an observation is that these are not yet a reality, leaving some pilot programmes aside. Therefore, as it stands, it is too early to tell whether CBDCs will indeed be(come) game changers for payments. More research needs to be done. An interesting line of thought in this context, that links CBDCs with compliance with laws, is that replacing truly anonymous, untraceable cash with a public, traceable CBDC, could theoretically mark the end of many money laundering and criminal activities, although from a political perspective such scenario is probably unlikely.

Stablecoins

Unlike CBDCs, **stablecoins** are not just a lab experiment; various examples are already in circulation. Most stablecoins have a local footprint. Recently, however, new stablecoin initiatives have emerged. The most important one is probably Facebook's Libra project. These new initiatives are built on top of existing, large and/or cross-border user bases. They have the potential to scale very quickly to achieve a global or other substantial footprint and are commonly referred to as **"global stablecoins"**. Global stablecoins could provide various benefits to the financial system, most notably by lowering transaction fees in retail cross-border payments and facilitating financial inclusion, yet their global scale also poses new challenges and risks to, amongst others, financial stability and monetary policy.

Stablecoin types



Source: Created by the authors; based on ECB Occasional Paper Series No. 230 by D. Bullmann, J. Klemm and A. Pinna[3].

Global stablecoins are not the only regulatory concern the legislator faces today. Another concern is that, at present, EU financial laws do not prohibit financial institutions from holding or gaining exposure to crypto-assets or from offering services relating to crypto-assets. This can prove problematic: most crypto-assets exhibit a high degree of **volatility** or have not yet proven to be truly resilient in times of financial stress. In other words, if financial institutions decide to acquire them and take them on their balance sheets or engage in activities that involve them, they could face enormous losses. As part of a conservative prudential treatment, for now, the best way forward to deal with the uncertainty surrounding crypto-assets, is probably to deduct them from a financial institution's own funds. A continuing concern is, moreover, the use of crypto-assets for financial crime. Crypto-assets pose serious money laundering and terrorist financing risks that criminals, money launderers, terrorists and other illicit actors could exploit. The fact that they are **fully digital**, easily transferable, pseudonymous – and with the use of specific anonymity-enhancing technology even completely anonymous – assets that operate on a decentralised basis, makes them particularly suitable for money laundering and other criminal activities.

Anti-money laundering / Combatting the financing of terrorism

To address the ML/TF risks presented by cryptocurrencies - or, as the EU up until now referred to them, "virtual currencies" - the EU legislator included so-called "*custodian wallet providers*" and "*providers engaged in exchange services between virtual currencies and fiat currencies*" within the scope of the Anti-money laundering / Combating the financing of terrorism (AML/CFT) framework by defining them as obliged entities in AML Directive 5. However, since the adoption of AMLD5 on 30 May 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 Financial Action Task Force (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. 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. The FATF also adopted new Guidance on the application of the risk-based approach to virtual assets and virtual asset service providers in June 2019. A side-by-side comparison of the latest FATF standards on virtual assets with the AML/CFT-regime for virtual currencies set-out in AMLD5 shows that the existing European AML/CFT-regime for virtual currencies already lags behind of what is considered the current international AML/CFT-standard for crypto-assets.

Regulatory actions

To bring the European AML/CFT framework up to speed with the current reality in the crypto-space, the EU could consider a number of regulatory actions:

1. Broaden the scope

A first regulatory action to consider is to **broaden the scope** of the definition of virtual currencies, for instance to include tokens.

2. Broaden the list of obliged entities

The list of **obliged entities** could be broadened. The following blind spots could be addressed:

- crypto-exchanges exchanging crypto into crypto;
- financial service providers who are active in the participation in and provision of financial services related to an issuer's offer and/or sale of a crypto-asset; and
- trading platforms, at least insofar they are centrally operated.

An interesting question is whether it would not also make sense to include issuers or offerors of crypto-assets into the list of obliged entities. Non-custodian **wallet providers** only provide the technical tools for others to work with and typically do not function as an intermediary so it does not make much sense to target them for AML/CFT purposes. The same holds true for coin inventors.

A different approach is warranted for **miners**. Nowadays, 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. As it stands, such rigs can be set up by anyone, even criminal actors. 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 crypto-assets, the resulting funds are also clean. A first regulatory step could be to try to map the use of this technique and subsequently, if it effectively proves an important blind spot, to consider appropriate counter measures.

In addition, and in view of the cross-border nature of crypto-assets and their misuse, the introduction of a **European AML 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. When enhancing the regulatory framework with respect to criminal use of crypto-assets, the EU should be mindful to also enhance the investigative toolbox: to ensure compliance with the regulatory framework, law enforcement agencies must be able to detect infractions and subsequently sanction them. Therefore, the EU should continue to invest in initiatives that add to the investigative toolbox of law

enforcement agencies who are trying to track down ML/TF and other illicit activities such as tax evasion via crypto-assets.

3. Investments in crypto-assets

A third regulatory concern relates to **investments** in crypto-assets. Since the explosion of initial coin offerings in 2017, various regulators have issued statements warning people that investments in crypto-assets are very risky and often fall outside the scope of EU financial services laws, leaving investors unprotected if something goes wrong. At the same time, regulators have pointed out that, depending on the specific design features of crypto-assets, they can be included in the scope of EU financial services laws. In practice, however, it is not always clear if a crypto-asset effectively falls inside the scope of the existing regulatory framework. This is not only due to the often tailored nature of crypto-assets, but also to the lack of clarity in the financial regulatory framework. These circumstances are challenging for all actors involved (including financial supervisors, crypto investment firms and crypto investors), contribute to regulatory arbitrage and generally lead to legal uncertainty.

To create a level playing field and ensure adequate investor protection across the EU, a common view on the legal qualification of crypto-assets as financial instruments is required. Moreover, EU financial services laws should be brought up to speed with the unique characteristics of the crypto-sector, to allow for an effective application of the existing financial regulation to crypto-assets that are financial instruments. As regards crypto-assets that do not qualify as MiFID II financial instruments, nor EMD2 electronic money, and hence, escape all EU financial regulation, the EU should, at the very least, put appropriate risk disclosure requirements in place, so that investors and/or consumers can be made aware of the potential risks prior to committing funds to these crypto-assets.

4. Cybersecurity

A last regulatory concern considered in this study is **cybersecurity**. Cybersecurity has become a major issue in the field of crypto-assets. Stolen crypto-assets typically find their way to illegal markets and are used to fund further criminal activity. Along the same lines, in the context of ransomware attacks, criminals often ask victims to pay the ransom in cryptocurrencies such as Bitcoin. Cryptocurrencies allow criminals to monetise on ransomware attacks without revealing their real-life identities, making such attacks very interesting and lucrative exploits. In the current state of the EU regulatory framework, there are no specific laws that set-out minimum standards for cybersecurity to be complied with by intermediaries who offer custodial services for crypto-assets. The EU should consider introducing such standards for intermediaries operating within the EU. To decrease the number of successful ransomware attacks involving crypto-ransoms, overall cyber-security awareness can be improved. In addition, a regulatory response could be to make it harder for criminals to use the crypto-ransoms they have collected for other, future, transactions. This could be done by blacklisting the coins used to pay a crypto-ransom.

---

1 https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf

2 https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

3 Bullmann, D., Klemm, J. and Pinna, A., "In search for stability in crypto-assets: are stablecoins the solution?", *ECB Occasional Paper No. 230*, August 2019, 10 (electronically available via https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf)

Disclaimer and copyright. The opinions expressed in this document are the sole responsibility of the authors and do not necessarily represent the official position of the European Parliament. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy. © European Union, 2020.
© Image on page 1 used under licence from Shutterstock.com

IP/A/ECON/2020-23; Manuscript completed: April 2020; Date of publication: May 2020
Administrator responsible: Dirk VERBEKEN; Editorial assistant: Janetta CUJKOVA
Contact: Poldep-Economy-Science@ep.europa.eu
This document is available on the internet at: www.europarl.europa.eu/supporting-analyses

Print ISBN 978-92-846-6562-4 | doi:10.2861/656571 | QA-04-20-241-EN-C
PDF ISBN 978-92-846-6563-1 | doi:10.2861/814644 | QA-04-20-241-EN-N