



Finance Watch

Making finance serve society


One born every minute: Striking the balance between promoting innovation and protecting citizens

An analysis of the EU Digital Finance package

A Finance Watch report



October 2021



“Distributed ledger technology (DLT) is full of potential. To harness this potential in a way that is safe and beneficial for its users, we have to build upon robust regulation.”

Author: Christian M. Stiefmueller

Editors: James Pieper

Cover photo: Adobe Stock / © metamorworks

Graphics and typeset: Camila Dubois

© Finance Watch 2021

The contents of this report may be freely used or reproduced without permission provided the original meaning and context are not altered in any way. Where third party copyright has been acknowledged, permission must be sought from the third party directly. For enquiries relating to this report, please email contact@finance-watch.org.

Finance Watch has received funding from the European Union to implement its work programme. There is no implied endorsement by the EU or the European Commission of Finance Watch's work, which remains the sole responsibility of Finance Watch.



Co-funded by
the European Union

Contents

A. Proposal for a Regulation of the European Parliament and the Council on Markets in Cryptoassets ('MiCA')	4
1. Need for regulatory action	4
2. Scope and definitions	5
2.1. 'e-money tokens'	5
3. Markets and market participants	8
4. Regulatory perimeter	9
5. Preliminary summary	10
6. Regulation of crypto-assets: an 'incremental' approach	11
6.1. General principles	11
6.2. Classification of crypto-assets	11
B. Proposal for a Regulation of the European Parliament and the Council on Digital Operational Resilience ('DORA')	15
1. Scope: coverage and relationship with other EU legislation	15
2. Substantive legislation	15
2.1. ICT governance and risk management	15
2.2. Incident reporting and information sharing	16
2.3. Operational resilience testing	16
2.4. ICT third-party risk	17
3. Supervision: structures and processes	17
C. Proposal for a Regulation of the European Parliament and the Council on a Pilot Regime for Market Infrastructures based on Distributed Ledger Technology ('DLT Pilot')	18
1. Regulatory approach	18
2. Eligible financial instruments	19
3. Direct access to retail investors	19
4. Role of DLT network nodes (validators)	20
5. Relationship with DORA	20

A. Proposal for a Regulation of the European Parliament and the Council on Markets in Cryptoassets ('MiCA')

1. Need for regulatory action

The market for crypto-assets has seen phenomenal growth: when the first Bitcoin was issued in January 2009, it set off an avalanche of new issues. As of today, more than 12,500 crypto-assets with a total reported value in excess of USD 2.3 trn are in circulation.¹ On the other hand, nearly 2,300 crypto-asset projects are reported to have failed already.² They fail for a variety of reasons: unsuccessful projects are abandoned by their sponsors, others hacked, but nearly one in three projects are thought to be linked to outright fraud³. In many instances, retail investors were among those affected.

The announcement by Facebook, in June 2019, of its plan to launch a global payment system based on the Libra (now: Diem) stablecoin has lifted the debate surrounding crypto-assets to a new level. Billed by its promoters as a new way for users to make digital payments, cheaply and conveniently, Libra/Diem seeks to leverage Facebook's global user base of 2.9 billion⁴. The presentation of Libra/Diem has added new urgency for governments to update their legal frameworks to account for stablecoins and other categories of crypto-assets, and for central banks to advance their own plans for "central bank digital currencies" (CBDCs).

Unlike other major jurisdictions, the European Union has taken the initiative to regulate and supervise this emerging market. In its proposal for a Regulation for Markets in Crypto-assets (MiCA)⁵, the Commission sets out three main goals: protecting investors and users, preserving financial stability, and preventing any dilution of central banks' control of monetary policy. Finance Watch welcomes the legislative proposal and supports Commission objectives.

Throughout the proposal, the Commission emphasises that it intends to proceed cautiously so as to not hinder innovation in a still emerging field of technological and commercial development. Finance Watch agrees that regulation must be balanced carefully and should not stand in the way of genuine innovation and its potentially substantial societal benefits. This balance is clearly difficult to strike but should ultimately favour the common good over vested commercial interests. In a number of instances, the proposal offers room for improvement in this respect.

1 [CoinMarketCap, Today's Cryptocurrency Prices by Market Cap](#), as of 30 September 2021.

2 [Coinopsy, List of Dead Crypto-Coins](#), as of 30 September 2021.

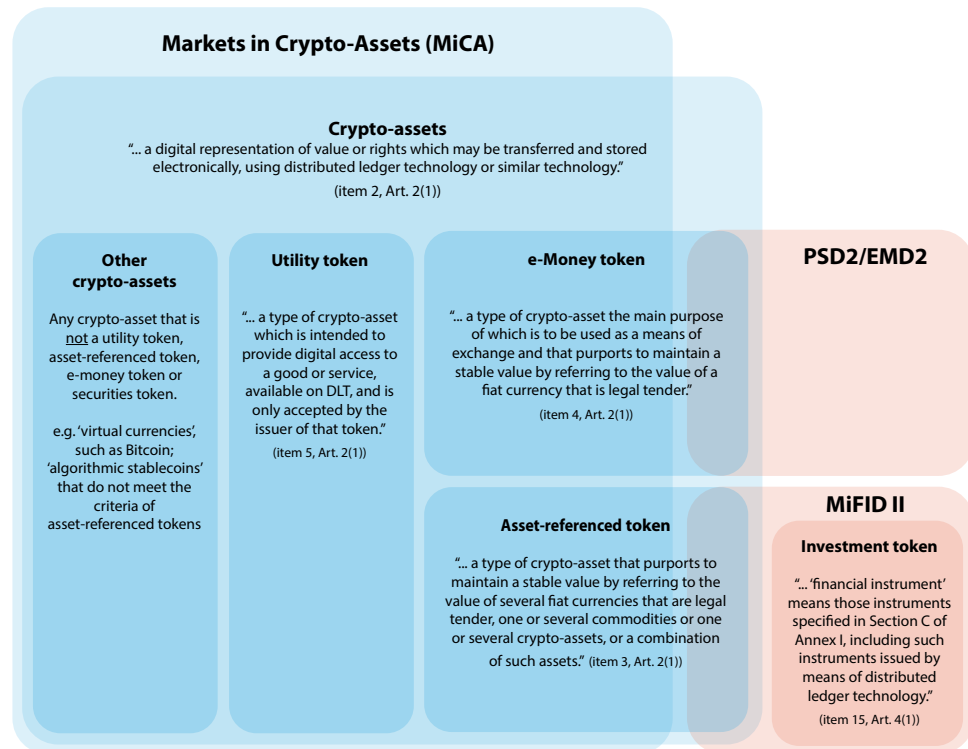
3 Chen Zhehao, [2019 had 20% Fewer Dead Crypto Projects Than the Year Before](#), 07 January 2020.

4 [Facebook Inc., Earnings Presentation Q2 2021](#).

5 Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, COM(2020) 593 final, 24 September 2020.

2. Scope and definitions

MiCA does not provide an exhaustive taxonomy of instruments that do, or do not qualify as crypto-assets. It does, however, attempt to define a number of categories that pose specific risks and therefore require stricter regulation. The proposed categorisation still has a number of issues and does not make sufficient use of existing, largely complementary financial sector legislation.



2.1. 'e-money tokens'

The proposal recognises that a privately issued token based on an existing fiat currency is not substantively different from electronic money under the Revised Electronic Money Directive (EMD 2)⁶. It therefore limits the right to issue "e-money tokens" in the EU to credit institutions, authorised under the Capital Requirements Regulation and Directive (CRR II/CRD V)⁷, and e-money institutions, authorised in accordance with EMD 2. The features of "e-money tokens" are also aligned with the provisions of the Revised Payment Services Directive (PSD 2)⁸ and EMD 2. In particular, they must provide the tokenholder with a legal claim against the issuer and be redeemable at par at all times (Art. 44(1) MiCA and Art. 4(25) PSD 2). For the avoidance of doubt, "e-money tokens" based on an EU currency should be defined unequivocally as "electronic money" within the meaning of Article 2(2) EMD 2.

⁶ Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions, OJ L 267/2009, pg. 7.

⁷ Regulation (EU) 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms, OJ L 176/2013, pg. 1; and Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, OJ L 176/2013, pg. 338.

⁸ Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, OJ L 337/2015, pg. 35.

The adoption of non-cash payments, including both traditional channels, such as bank transfers, credit and debit cards, and electronic channels, is progressing in all EU member states. Across member states this process unfolds in different ways, and at different speeds⁹, with incumbents, in particular banks and major global card providers, continuing to play a dominant role. In addition to legislative and regulatory initiatives towards harmonisation, such as the Single Euro Payment Area (SEPA)¹⁰, increased competition, including from providers of new, digital payment solutions, is expected to increase the choice for customers, promote the adoption of instant payments, and bring down the cost of cross-border payments and remittances. Finance Watch supports these objectives.

It should be noted, however, that initiatives aimed at increasing competition – such as “Open Banking”, introduced with PSD 2 – are likely to raise new issues in turn. On the one hand, the quest for a more competitive market should not compromise the level of protection afforded to customers. As the market for payment services – tokenised or other – is opened to new entrants, including start-ups with limited resources and operating history, policymakers and regulators should ensure that all market participants are subject to appropriate licensing, prudential regulation, and supervision. Recent events, such as the Wirecard case, have highlighted regulatory shortcomings that must be addressed as a matter of urgency.¹¹ Any forthcoming review of the PSD 2/EMD 2 framework should comprise a careful evaluation and harmonisation of the regulatory perimeter, and more stringent prudential requirements for payment institutions.

On the other hand, the “unbundling” of the value chain in payments, initiated by PSD 2, could also pave the way for large digital platform providers to leverage their customer relationships and Big Data capabilities to become dominant “gatekeepers” in this market. Policies that facilitate the emergence of new dominant players in a marketplace that has been struggling historically with concentration and competition issues are ultimately counterproductive.¹² “Open Banking”, in its current form, favours these platform providers and their “data-centric” business models. A review of the PSD 2/EMD 2 framework should aim for closer alignment with the letter, and spirit, of the General Data Protection Regulation (GDPR)¹³ and follow a “user-centric” approach based, in particular, on the principles of purpose limitation, data minimisation, fairness and transparency. In conjunction with other legislative initiatives, such as the proposed Digital Markets Act (DMA)¹⁴, it should result in a more robust and effective regulatory framework, especially for large digital platform providers.

9 European Commission, [Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on a Retail Payments Strategy for the EU](#), COM(2020) 592 final, 24 September 2020, pg. 13.

10 Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in Euro, OJ L 094/2012, pg. 22.

11 European Securities and Markets Authority, [Fast Track Peer Review on the Application of the Guidelines on the Enforcement of Financial Information \(ESMA/2014/1293\) by BAFin and FREP in the Context of Wirecard: Peer Review Report](#), ESMA42-111-5349, 03 November 2020.

12 Stiefmueller, Christian, [Open Banking and PSD 2: The Promise of Transforming Banking by “Empowering Customers”](#), in: Spohrer Jim / Leitner, Christine (eds.), *Advances in the Human Side of Service Engineering*. (AHFE 2020, *Advances in Intelligent Systems and Computing*, vol 1208 (2020), Springer Cham, pg. 299.

13 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, OJ L 119/2016, pg. 1.

14 Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector, COM(2020) 842 final, 15 December 2020.

2.2. 'Asset-referenced tokens'

In Art. 3(1) MiCA, “asset-referenced tokens” are defined as *“a type of crypto-asset that purports to maintain a stable value by referring to the value of several fiat currencies that are legal tender, one or several commodities or one or several crypto-assets, or a combination of such assets.”* This definition contains two major flaws, one semantic, the other systematic:

- Semantically, an “asset-referenced token” only needs to *“purport to maintain a stable value”*. The term “asset-referenced”, as opposed to “asset-backed”, in combination with the absence, in Art. 32 MiCA, of an explicit requirement to maintain a reserve of assets at all times that is equal or greater than the nominal value of tokens in issue, and the absence, in Art. 35 MiCA, of a statutory right for holders of “asset-referenced tokens” to redeem their tokens at any time, affords issuers of “asset-referenced tokens” discretion in deciding how much reserve they intend to hold and whether investors would have any claim or redemption rights on the issuer or the reserve assets. This degree of latitude would be, in our view, excessive: if “asset-referenced tokens” are to be *“widely adopted by users to transfer value or as a means of payments”*, as the proposal purports (recital 25), it is essential for them a) to be “asset-backed” in full, and b) to ensure that holders may claim, and can obtain redemption of their holdings at all times.
- Systematically, the vague definition of an “asset-referenced token” does not conform to the basic principle of “same business, same risk, same rules”, which purportedly informs the regulatory approach, in MiCA and throughout the Digital Finance Package. If the token is fully backed by assets, as it should be to fulfil its purpose (see above), it becomes, for all intents and purposes, the digital equivalent of a “unit” in a collective investment undertaking, such as a money market fund (MMF), unit trust (UCITS) or alternative investment fund (AIF). If the token is “referenced” in any other way to one or more underlying assets, such as currencies or commodities, its value is more loosely derived from that of the underlying asset, which tends to be the defining characteristic of a “derivative”. According to Section C of Annex I of the 2nd Markets in Financial Instruments Directive (MiFID II)¹⁵ derivatives on currencies and commodities are “financial instruments” for regulation purposes. Under the proposed amendment to Art. 4(1) MiFID II, a tokenised derivative should be considered as a “financial instrument”, obviating the need for a new category.
- As for the latter, Finance Watch notes that derivatives tend to be strictly regulated due to their particular risks. The UK financial markets supervisor, the Financial Conduct Authority (FCA), has recently issued a regulation banning the sale of derivative investment products referenced to crypto-assets to retail investors¹⁶. The FCA noted, in particular, the *“inherent nature of the underlying assets, which have no reliable basis for valuation, [the] presence of market abuse and financial crime [...] in the secondary market for crypto-assets, [the] extreme volatility in crypto-asset prices movements as well as the “inadequate understanding by retail consumers of crypto-assets and the lack of a clear investment need for investment*

¹⁵ Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments, OJ L 173/2014, pg. 349.

¹⁶ Financial Conduct Authority, [Prohibiting the sale to retail clients of investment products that reference cryptoassets. Policy Statement PS/20/10](#), 06 October 2020.

*products referencing them.*¹⁷ Finance Watch concurs with the FCAs view on the questionable contribution of this category of products to financial innovation and the functioning of financial markets.

For the purposes of regulatory consistency, the definition of “asset-referenced tokens” should ideally be removed from the text. There is, to our knowledge, little evidence to suggest that these instruments should not be considered as tokenised “financial instruments” that would either fall into one of the existing categories of Section C of Annex I of MiFID II, or could be readily added to that list. The latter would be the case, in particular, for tokens that are referenced to other crypto-assets.

Alternatively, the definition of “asset-referenced tokens” (Art. 3(1) MiCA), the requirements regarding the reserve fund in (Art. 32), and tokenholders’ rights towards the issuer and/or the reserve (Art. 35) should be amended so as to ensure that tokens in issue are fully backed by reserve assets, and redeemable by tokenholders, at all times. “Asset-referenced tokens” that do not fulfil these requirements should not be eligible to be offered to retail investors/users in the European Union. Moreover, as the prohibition for issuers or service providers to pay interest on “asset-referenced tokens” (Art. 36 MiCA) or “-e-money” tokens (Art. 45 MiCA) seems to clearly indicate, these tokens should not be considered as “deposits”, e.g. for the purposes of the Deposit Guarantee Scheme Directive¹⁸. “White papers” issued in connection with such tokens should explicitly warn users that depositor protection does not apply (Art. 17 MiCA).

3. Markets and market participants

MiCA establishes a “light touch” regulatory framework for issuers and service providers that foregoes many of the safeguards attached to comparable activities in the analogue sphere. By contrast, other important roles that are unique to DLT are hardly regulated at all. There is a need to revisit the proposed balance between encouraging innovation and experimentation, on the one hand and ensuring uniform high standards of professionalism and governance among industry participants, on the other.

MiCA endeavours to regulate not only the issuers of crypto-assets but also the providers of related services. It could be argued that many, if not most of these services, and service providers, are already well-defined, and regulated in some detail, in other financial services legislation, such as MiFID II, PSD 2 and EMD 2. This applies, for instance, for brokers, trading venues, asset managers and custodians. Sections A and B of Annex I of MiFID II comprise lists of “investment services and activities” and “ancillary services” in relation to financial instruments. As mentioned in Section 2 above, many “asset-referenced tokens” could be regarded as tokenised “financial instruments”. On this basis, the framework governing “investment services” and “ancillary services” under MiFID II would be applicable and provide a mature, tried and tested basis for regulating a significant part of the evolving service ecosystem. This would not stop regulators, in our view, from making adjustments that cater to the peculiarities of tokenised financial instruments.

¹⁷ see Note 16 above.

¹⁸ Directive 2014/49/EU of the European Parliament and of the Council of 16 April 2014 on deposit guarantee schemes, OJ L 173/2014, pg. 149.

Other roles, such as “validators”, by contrast, are specific to the DLT environment and would require separate consideration by regulators. So far, MiCA and the proposed DLT Pilot Regulation¹⁹ have been largely silent on any requirements for “validators”, except to say, in Art. 6(2) DLT Pilot Regulation, that central securities depositories (CSDs), investment firms or marketplace operators running a DLT-based securities settlement system, or trading facility (MTF) need to *“establish rules on the functioning of the DLT they operate, including the rules for accessing the distributed ledger technology, the participation of the validating nodes, addressing potential conflicts of interest, and risk management including any mitigation measures”*. Similarly, issuers of “asset-referenced tokens” have to formulate governance arrangements for the validation process and disclose them in their “crypto-asset white paper” (Art. 21(1) and 30(5) MiCA). It is important to note, however, that the soundness and integrity of the validation process is vital for the functioning of a DLT infrastructure: the obligation to design, disclose and implement adequate governance arrangements should therefore apply to all issuers of crypto-assets. General obligations to that effect should be included in Art. 5(1) and 13 MiCA.

4. Regulatory perimeter

The principal objective of regulating this market is to protect investors and other users, and to preserve financial stability in the European Union. Implementing these safeguards effectively is difficult in a market whose foundational technology (DLT) is distributed by design and whose reach is inherently global. EU legislation should be guided, first and foremost, by the obligation to protect European citizens and users, and by the need to secure a level playing field for EU-based issuers and service providers.

The objective of MiCA is to provide a harmonised level of protection to all users of crypto-assets in the Union. MiCA is designed to apply to issuers of crypto-assets in the EU and providers offering services related to crypto-assets in the European Union (Art. 2(1) MiCA). The principal criterion is whether the asset is available in the Union, which implies that issuers and service providers who are not EU-based, but offer products or services to EU-based clients, fall under its jurisdiction. In respect of “e-money tokens”, Art. 43(1) states expressly that any token that *“references a Union currency shall be deemed to be offered to the public in the Union”*.

The regulation does not explicitly require non-EU issuers to establish a presence in the European Union. It does, however, require issuers of crypto-assets other than “e-money” and “asset-referenced tokens” to be a legal entity (Art. 4(1) MiCA) and to notify the “crypto-asset white paper” to the competent authority of their *“home Member State”* (Art. 8 MiCA). According to Art. 43(1) MiCA, only credit institutions or electronic money institutions that are licensed and authorised in the European Union under the relevant legal framework are permitted to issue “e-money tokens”.

All crypto-asset service providers, as well as issuers of “asset-referenced tokens”, are obliged to have a registered office in the European Union (Art. 15(2) and 53(1) MiCA). Once registered in one EU member state, service providers would benefit from a “passporting” regime that would allow them to operate across the EU single market.

¹⁹ Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology, COM(2020) 594 final, 24 September 2020.

With these provisions, MiCA does not explicitly stake a claim to expand its regulatory perimeter outside the Union. It does, however, set out requirements for issuers and service providers who intend to operate on the EU market that should bring most crypto-assets that are legally marketed to EU-based users under the protection of EU law.

Finance Watch notes that the proposal does not differentiate between the “issuer” and the person or entity who offers the crypto-asset to potential users in the European Union (the “offeror”). It is important to recognise that these are separate roles and each should be regulated accordingly. For crypto-assets that are issued by non-EU persons or entities or crypto-assets that do not have a known issuer, such as Bitcoin, the offeror plays a critical role and should bear responsibility vis à vis EU authorities and users, especially for observing investor protection and market conduct rules. It should therefore be required to have a legal, and physical presence in the European Union.

“Global stablecoins” require strict oversight at the EU level. In line with policymakers’ concern about the emergence of “global stablecoins” that could challenge the monetary sovereignty of governments and central banks, MiCA defines stablecoins – issued in the form of “e-money tokens” or “asset-referenced tokens” – as “significant” if they fulfil at least three of the criteria set out in Arts. 39(6) MiCA (Art. 39(1) and 50(1) MiCA).

Under the proposal, authorisation of a “significant” token may be granted ex-ante, upon application by the issuer to the relevant national competent authority before tokens are placed on the market (Art. 40 MiCA), or ex-post, if a token already in circulation meets or exceeds the threshold values (Art. 39(3) MiCA). In both instances, the decision to approve or reject the application is made by European Banking Authority (EBA), in close coordination with the national competent authority.

Issuers of “significant asset-referenced” tokens would be supervised by the EBA, while issuers of “significant e-money” tokens would be supervised jointly by the authority and the national competent authority. Regarding the latter, Finance Watch would question whether it is practical to assign overlapping mandates to the national regulator and EBA – it may be preferable to concentrate supervisory responsibilities at the latter in both instances.

The proposed framework goes some way towards setting a global standard. Questions remain, however, regarding the effective enforcement of EU rules in respect of “significant” tokens that are issued by third-country entities and traded globally. This is likely to depend largely on continued constructive engagement between the European Union and other major jurisdictions in the relevant international fora, such as the Financial Stability Board (FSB) and the Committee on Payments and Market Infrastructures (CPMI) at the Bank for International Settlements (BIS).

5. Preliminary summary

At this stage, pending further analysis and discussions with the Commission, policymakers and other stakeholders, Finance Watch would like to register some reservations concerning the MiCA proposal. Finance Watch welcomes the readiness of the EU institutions to create a firm legal foundation for users, issuers and providers but notes that the desire to maintain flexibility to accommodate further technological and commercial innovation comes at the expense of legal and regulatory consistency. There is room for improvement in defining and regulating the

boundaries towards existing regulatory frameworks, in particular MiFIR/MIFID II, PSD 2 and EMD 2. In particular, the absence of clear and unequivocal rules regarding the calibration of reserves and redeemability of “asset-referenced tokens” introduces the risk of creating leverage in the financial system that is not supported by adequate prudential requirements.

In its attempt to accommodate future innovation, the proposal lacks regulatory ambition in some respects and the principle of “same business, same risk, same rules” is not applied consistently. Specifically, tokens that effectively replicate existing financial instruments, which could be the case for a significant share of “asset-referenced tokens”, should unequivocally fall under existing financial services legislation to extend the benefits of the available protections for investors and customers.

Finance Watch does not purport to be in a position to foretell all developments in this rapidly evolving industry. The association is mindful, however, that financial innovation which adds to the complexity of the marketplace without offering demonstrable benefits for its participants all too often turns out to do more harm than good.²⁰ While it is in the interest of EU citizens and businesses that the regulatory framework remains flexible and open to useful, productive innovation, it is equally important for the legislator to set clearly defined limits to experimentation and to ensure that the high standards of market integrity and investor/customer protection that govern traditional, mature markets are maintained when setting rules for new, emerging ones.

6. Regulation of crypto-assets: an ‘incremental’ approach

6.1. General principles

Finance Watch is of the view that the regulatory framework for crypto-assets in the European Union should first and foremost protect the interests of individual and corporate users of financial services, and preserve financial stability. It should be consistent with, and build upon existing regulation, in particular MiFID II and PSD 2/EMD 2. Last, but not least, it should also be “future-proof” and resilient against “regulatory arbitrage”.

6.2. Classification of crypto-assets

In our view, there are six criteria that should govern the classification of crypto-assets/tokens:

- Is the token being offered to users in the European Union?
- Is there an identifiable issuer of the token?
- Is the token being issued against consideration? If so, what does the required consideration consist of: official (fiat) currency, financial assets, commodities, and/or other crypto-assets?
- Is the token fully backed up by collateral? If so, what does the collateral (reserve) consist of: official (fiat) currency, financial assets, commodities, and/or other crypto-assets?
- Does the tokenholder have a claim to redeem his/her token? If so, against whom/what: the issuer, the collateral (reserve), and/or a third party (e.g. a guarantor)?
- Finally, is the token traded in the European Union? If so, how is it traded: peer-to-peer (on-

20 “Philosophers and Quants” in: Finance Watch, [Ten Years After: Back to Business as Usual](#). Post-Crisis Financial Regulation in Europe, 15 September 2018, pgs. 16-17.

chain) or via an intermediary (via a broker or exchange).

According to the answers given above, crypto-assets that are issued against consideration could be categorised as follows:

- tokens that provide digital access to a good or service and are only accepted by the issuer of that token are “utility tokens”, according to the definition proposed by MiCA;
- “e-money tokens” are the tokenised equivalent of “e-money” and should be covered by EMD 2. EMD 2 would need to be amended selectively to cover specific aspects of tokenisation;
- “asset-referenced tokens” that provide a claim against a “reserve” (fund) of underlying assets could be considered as financial instruments (tokenised “money market instruments” or “units in collective investment undertakings”; items 2 and 3 of Section C, Annex I MiFID II) and could be regulated under MiFID II and the relevant regulations (MMF) and directives (UCITS and AIFM), which would need to be amended accordingly;
- “asset-referenced tokens” that provide an enforceable claim against the issuer could be considered as financial instruments. They could indeed be interpreted as a transferable debt obligation of the issuer (“transferable securities”; item 1 of Section C, Annex I MiFID II), except that the nominal amount of the obligation is not a fixed amount in official (fiat) currency but a variable amount determined by the market value of a reference asset or assets. MiFID II may need to be amended to cover specific aspects of tokenisation;
- the term “investment token” should be defined in MiFID II to identify and distinguish financial instruments that are issued in tokenised form.

Crypto-assets (with or without an identifiable issuer) that are not issued against consideration – against payment in official currency (“funds”) or in exchange for other assets (including crypto-assets) – will not normally qualify as “financial instruments”. They may still pose a financial risk for users, however, if they are a) offered for purchase (against consideration) by a crypto-asset service provider to EU citizens and/or b) traded (against consideration) by a crypto-asset service provider in the European Union. This category of crypto-asset “*sui generis*” (e.g. Bitcoin) should be regulated primarily in MiCA.

Provisions regarding the supervision of issuers of “significant” “e-money” tokens by the EBA (Chapter 2 of Title IV (Art. 50 to 52) MiCA) or “asset-referenced tokens” (Chapter 5 of Title III (Art. 39 to 42) MiCA) should be incorporated into the relevant framework. It should be noted that, in order to be effective, supervision should be applied to institutions (the issuers) not instruments.

The regulatory framework for crypto-asset service providers (CASPs) should follow the categorisation of the crypto-asset that the services relate to. Most of these services are already covered under relevant legislation, e.g. in Sections A and B of Annex I to MiFID II (for financial instruments, including “asset-referenced tokens”) and in PSD 2/EMD 2 (for payment instruments, including “e-money tokens”). For consistency, and to avoid a proliferation of parallel legal frameworks, crypto-asset service providers should be authorised under the relevant framework, i.e. as a credit institution, payment/e-money institution, and/or investment firm. The conditions for authorisation are set out in CRR II/CRD V, PSD 2/EMD 2, MIFIR/MIFID II, and the Investment Firms Regulation

and Directive (IFR/IFD), respectively, and would be applicable with only minor adaptations. The supervision of crypto-asset service providers would be governed accordingly.

There still remains a very real, and material risk of mis-selling. The regulatory approach implicit in MiCA is to cast the widest possible regulatory perimeter. That implies, however, that high-risk crypto-assets may still be offered to users in the European Union, subject only to limited formal prerequisites (Art. 4 MiCA), disclosures (Art. 5 to 11 MiCA), and legal liability (Art. 13 and 14 MiCA). Finance Watch therefore proposes the following recommendations to address these shortcomings:

- Crypto-asset white papers and other marketing communication (online and off-line), especially for crypto-assets that do not fall into one of the defined categories (“asset-referenced tokens”, “e-money tokens”, “utility tokens”, and “investment tokens”), should contain prominent warnings to potential users that these crypto-assets covered by an investor compensation or deposit guarantee scheme;
- If the crypto-asset is offered to the public by a person or entity other than the issuer, the offeror should be held legally liable for the completeness and accuracy of the information provided to potential users. In order to ensure that users are able to enforce potential claims for compensation, and that the offeror has the financial capacity to honour these claims, the offeror should be a) a legal entity domiciled in the European Union; and b) required to disclose adequate information on its financial position;
- Crypto-assets should be admitted to trading on a trading platform that is accessible to the general public only if the application has been made by a professional firm that is authorised for providing the relevant crypto-asset services under the supervision of a competent authority in an EU member state.

The soundness and integrity of the validation process is vital for the proper functioning of a DLT infrastructure. Particular consideration should therefore be given by regulators to the role of “validators”:

- In a permissioned DLT network, where the operators of DLT network nodes who participate in the consensus mechanism are known, these “validators” should be subject to specific obligations. Art. 6(2) DLT Pilot Regulation requires central securities depositories (CSDs), investment firms or marketplace operators running a DLT-based securities settlement system, or trading facility (MTF) to “*establish rules on the functioning of the DLT they operate, including the rules for accessing the distributed ledger technology, the participation of the validating nodes, addressing potential conflicts of interest, and risk management including any mitigation measures*”. Equally importantly, entities that operate a permissioned DLT network should also be required to comply with the provisions of the proposed regulation on Digital Operational Resilience for the Financial Sector (DORA).²¹
- In a non-permissioned DLT network, where the operators of DLT network nodes are widely dispersed and frequently anonymous, and the consensus mechanism is based entirely on

²¹ Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector, COM(2020) 595 final, 24 September 2020.

algorithmic processes (e.g. “proof-of-work”, “proof-of-stake”), certain (limited) obligations could be imposed on the offeror of the crypto-asset. In particular the offeror could be required to a) operate a DLT network node (“control node”) that comprises a full copy of the ledger; b) continuously monitor the operation of the DLT network for obvious disruptions and irregularities; and c) periodically, e.g. annually, commission an external report (“audit”) from a qualified third-party provider on the integrity of the DLT infrastructure and the proper operation of its governance arrangements and consensus mechanism.

B. Proposal for a Regulation of the European Parliament and the Council on Digital Operational Resilience ('DORA')

1. Scope: coverage and relationship with other EU legislation

DORA Regulation amends Credit Ratings Agencies (CCR) (1060/2009/EU), EMIR (648/2012/EU), MiFIR (600/2014/EU), and CSDR (909/2014/EU) Regulations.

DORA Directive amends Audit (EC/2006/43), UCITS (EC/2009/65), Solvency II (EU/2009/138), AIFMD (EU/2011/61), CRD IV (EU/2013/36), MiFID II (EU/2014/65), PSD 2 (EU/2015/2366), IORP (EU/2016/2341) Directives.

Relationship with the Network and Information Security (NIS) Directive: NIS (EU/2016/1148) sets out a “minimum harmonisation” framework for cybersecurity incident reporting, risk management and certification. It covers ICT services providers that are Operators of Essential Services (OES) or Digital Service Providers (DSP). OES are providers of essential ICT (“network and information”) services to certain designated sectors: Energy (electricity, oil, gas), Water Supply, Transport (air, rail, road, shipping), Finance (banking, financial markets infrastructures), Healthcare, and Digital Infrastructure (internet exchange points, DNS service providers, top-level domain name registrars). DSPs are providers of digital services, such as online marketplaces, online search engines, and cloud computing services.

According to Art 1(7) NISD and the EU institutions’ Communication on the implementation of the NIS Directive (“Making the Most of NIS”, COM/2017/0476), specific sectoral legislation (“*lex specialis*”) takes precedence over NISD (“*lex generalis*”). In the financial sector, several legislative instruments contain provisions related to cybersecurity risk management (PSD 2, MiFID II, and EMIR) and/or incident reporting (PSD 2) that are deemed at “*least equivalent in effect*” to the obligations set out in NIS.

2. Substantive legislation

2.1. ICT governance and risk management

The proposed ICT governance and risk management requirements (**Art. 4 to 14 DORA**) should be reviewed against the relevant provisions in PSD 2, MiFID and EMIR in order to align with “best practice” and achieve a maximum of harmonisation across sectors. References to the relevant provisions, including delegated acts, can be found in the NIS Communication (COM/2017/0476).

For bank prudential requirements: financial institutions’ incident reports, as well as the results of digital operational resilience tests under DORA, ought to be included in the **supervisory review and evaluation process (SREP)** framework (Art. 97 ff. CRD V). The operational risk framework in CRR II (Art. 312 ff.) may need to be amended accordingly. Mandates should be issued to the EBA to issue guidelines for competent authorities (CAs) regarding the assessment and calibration of potential **Pillar 2** guidance and requirements.

For global systemically important banks (G-SIBs): DORA should be reviewed for alignment with **BCBS 239**, a standard issued by the BCBS in January 2013 response to the rapidly rising frequency and severity of ICT incidents at major international banks. BCBS 239 has been in force since January 2016 and is applicable for all EU G-SIBs. As of last the BCBS progress report, issued in April 2020, none of the currently eight EU G-SIBs was found to be compliant (neither were the remaining 22 overseas G-SIBs). DORA would be an opportunity to bring the issue of non-compliance with BCBS 239 back on the EU legislative agenda and encourage EU G-SIBs to become compliant.

For bank recovery & resolution: financial institutions' incident reports, as well as the results of digital operational resilience tests under DORA, ought to be taken into account (by resolution authorities (RAs) in the context of recovery planning and resolvability assessments. Cross-references should be inserted into BRRD II regarding the assessment of “critical functions” in the context of recovery and resolution planning, resolvability assessment and the removal of impediments (Art. 2(1) item 35, 6, 10, 15, 16, 17 and 31 BRRD II). In particular, dependencies on ICT services (provided in-house or by third parties) that are not, or not readily substitutable, should be reflected in the resolvability assessment and, if necessary, remedied (Art. 17 BRRD II).

2.2. Incident reporting and information sharing

In the interest of preserving the highest standard of protection against the risk of systemic disruption, the proposed **incident reporting** rules (**Art. 15 to 20 DORA**) should be reviewed against, and aligned with the existing provisions in PSD 2, as appropriate and practicable. References to the relevant provisions, including delegated acts, can be found in the NIS Communication (COM/2017/0476).

Sharing of threat intelligence should be **compulsory (Art. 40 DORA)**. Financial institutions should be obliged to file reports of known threats to their NCAs and relevant ESA. The information could then be shared, confidentially and anonymously, if requested, through a central clearing house, e.g. the proposed EU Hub for Incident Reporting (**Art. 19 DORA**).

The collective interest in preventing systemic instability and wide-ranging harm to the financial system clearly outweighs any individual institution's interest in protecting commercial secrets or preventing damage to its reputation. Proper mechanisms for the confidential exchange and handling of incident data should be put in place to mitigate the risk of leaks and reputational risk to institutions.

2.3. Operational resilience testing

Operational resilience testing should be carried out uniformly across all segments of the financial services sector and **implemented centrally** by the competent EU authority (ESA), in analogy to EBA's role in banking sector stress tests. All testing should follow the **same rules and procedures**. These should be agreed and issued by the **Joint Committee** rather than by the ESAs individually (**Art. 23(4) DORA**).

On a more general note, it is questionable whether the ESAs are indeed best placed and equipped to carry out such testing. Other EU agencies, such as ENISA, should have ready access to specialist resources with experience in testing and certifying ICT infrastructures and processes, which could probably be called upon for this purpose (see also C. below).

2.4. ICT third-party risk

Provisions on third-party ICT risk management, contracting and concentration risk (**Art. 25 to 27 DORA**) are per se useful but should be monitored and enforced by competent and resolution authorities under the existing supervisory mandates, e.g. for banks as part of SREP and recovery planning and resolvability assessments (see also B.1. above). This approach would ensure that the information obtained through this process, the assessment of financial firms' compliance, and any risks related thereto can be incorporated seamlessly into the relevant supervisory processes.

3. Supervision: structures and processes

It is unclear how this section (**Art. 28 to 39 DORA**) relates to a) the rest of this document and b) the NIS framework. DORA addresses issues that relate to financial-sector firms while this section expands the ESAs' supervisory mandate to ICT companies providing services to the financial sector.

Supervisory role of ESAs (Art. 28(1) DORA): under the current proposal, all three ESAs would effectively become supervisors of ICT service providers. Their mandate would, however, be limited a) to critical third-party-service providers (CTPPs), and b) to the part of CTPPs' business activity that provides services to the financial sector. In parallel, ICT service providers would still remain subject to Member State supervision under NIS if they are considered as Operators of Essential Services (OES) or Digital Service Providers (DSP). As a result, the same ICT services provider may become subject to supervision by the ESAs, on the one hand (as CTPP under DORA), and Member State ICT supervisory authorities (as OES or DSP under NIS). In our view, it is doubtful if this role is a) covered by the ESA's mandate, and b) conducive to the broader effort to establish uniform cybersecurity rules for essential sectors and enforcing these rules consistently across the Union.

Designation of critical third-party-service providers (CTPPs) (Art 25(2) DORA): apart from potentially duplicating efforts undertaken elsewhere (see above) it is worth questioning why all three ESAs should become involved in the supervision of ICT service providers. Instead of creating parallel structures that are, at best, wasteful and could, at worst, lead to inconsistencies in supervisory practice, it would be preferable to create one joint centre of competence for all three.

Again, from a structural point of view it would appear preferable to integrate the CTPP mandate with other, horizontal legislation, such as NIS. Arguably, the designation process under Art. 25 DORA, as well as the supervisory powers under Art. 31 DORA, would be applicable to the ICT services sector more generally and should perhaps be implemented, on a wider scale. The proposal for a **revised NIS Directive (NIS 2)**, published by the Commission on 16 December, 2020 (COM/2020/823 (final)), already envisages a significant expansion of its scope, adding eight new vertical sectors to the existing seven. To implement such a regime effectively the supervisory structure under NIS/NIS 2 and the set-up of ENISA may need to be further reviewed, however.

C. Proposal for a Regulation of the European Parliament and the Council on a Pilot Regime for Market Infrastructures based on Distributed Ledger Technology ('DLT Pilot')

1. Regulatory approach

On a general note, Finance Watch has been critical in the past of the concept of “regulatory sandboxes” and continues to view the approach with scepticism. Preferably, the roll-out of new technologies, such as DLT, should take place as much as possible within the existing legislative frameworks. Finance Watch subscribes to the principle of “technology neutrality” and fully supports the view that new, emerging technologies should not face obstacles that impede their adoption and/or unfairly favour entrenched competition. At the same time, however, there is no need to deliberately tilt the “level playing field” in favour of newcomers in the name of promoting innovation at all cost, in particular if this involves potentially compromising financial stability and/or the protection of investors.

That said, Finance Watch remains aware that the Central Securities Depositories Regulation (Regulation (EU) 909/2014; CSDR), in conjunction with the Markets in Financial Instruments Directive (Directive 2014/65/EU; MiFID II) and Regulation (Regulation (EU) No 600/2014; MiFIR), contains a number of formal requirements and arrangements that are specific to the “traditional” technologies used in securities trading and settlement, and which may indeed complicate the adoption of DLT technology in this area. Finance Watch would therefore support the proposed DLT Pilot framework as long as:

- it is confined to a specific segment of the market where the economic risk for market participants, and the risk of systemic disruption to the financial system, e.g. as a result of potential technical failures, remains limited; and
- it does not seek to lower existing standards of market conduct and investor protection, potentially setting a precedent that could encourage regulatory arbitrage and undermine the standards applicable in “traditional” markets.

Another caveat to be added to our support of “technology neutrality” is the condition that new technologies should, on balance, mark progress in terms of sustainability vis à vis their predecessors. One telling example would be the deployment of first-generation DLT technology based on the “proof of work” consensus mechanism, which is used, in particular, when “mining” Bitcoin. Recent estimates put the annualised energy consumption of the global Bitcoin infrastructure at ca. 80-90 TWh²², which would correspond approximately to the annual electricity consumption of Belgium or Finland. Other, less-energy intensive consensus mechanisms, known as “proof of stake”, exist and should be deployed instead. In the context of MiCA, Finance Watch argues therefore that crypto-assets which operate on a protocol that uses a “proof-of-work” mechanism

²² Mid-point estimate of the Cambridge [Bitcoin Electricity Consumption](#) Index (CBECI) and the [Bitcoin Energy Consumption](#) Index (BECI) as of 30 June 2021.

should not be authorised to be issued in the European Union, and trading of such assets in the Union should be discouraged.

2. Eligible financial instruments

Finance Watch broadly agrees with the proposed choice of eligible financial instruments. These categories are by no means low-risk instruments, however, due in part to the very same characteristics – small issue sizes and low liquidity – that make them suitable for experimentation under the pilot framework. Mindful that one of the underlying concerns is the so far unproven ability of DLT infrastructures to handle high volumes of transactions in a reliable and timely manner, Finance Watch would therefore suggest adding a third eligibility criterion based on a historical metric of average trading volume (new point (c) in **Art. 3(1) DLT Pilot**). Only securities whose daily trading volume over, e.g., a six-month to one-year historical reference period did not exceed a level that is, from today's perspective, safely handled by DLT. ESMA could be mandated to assist in setting an appropriate threshold value.

3. Direct access to retail investors

The proposal suggests that the provisions in MiFID II that restrict access to MTFs to professional intermediaries could be disapplied so that retail investors have direct access to the trading venue, provided that they are “*of sufficiently good repute*” and “*fit and proper*”, and have “*sufficient level of ability, competence, experience and knowledge of the post-trading and the functioning of the DLT*”. (Art. 5(4) DLT Pilot). This is being justified with the argument that many crypto-asset trading platforms already offer retail investors direct access and this arrangement would merely replicate these arrangements. Finance Watch do not agree with this reasoning:

- the securities that are eligible for trading under this pilot scheme carry a considerable level of risk – they include shares in small, illiquid companies, a segment that has always been difficult for retail investors to navigate, and frequently associated with “penny stock” scams;
- the proposed exemption from disintermediation would deprive retail investors of the protections provided under Section 2 of Chapter II (Art. 24 to 30) of MiFID II, notably the obligation for intermediaries to assess appropriateness/suitability. Investors could be directly exposed to high-risk investments without appropriate safeguards, and with little, if any, hope of seeking redress – from intermediaries, let alone issuers – in the event of misrepresentation or fraud;
- the argument that existing crypto-asset trading venues allow retail investors to trade in instruments that may be at least as risky as the securities that would be eligible under the DLT Pilot, without the protections of MiFID II, is beside the point. The ambition of the Digital Finance package, and the proposed Markets in Crypto-assets Regulation (COM 2020/593 final; MiCA) in particular, should be, to create the kind of regulated environment that enables investors, including retail investors, to trade in “tokenised” instruments – transferable securities or other – with the same level of confidence they enjoy under the existing regulatory framework when trading “traditional” assets. This legislative effort should be seen as an exercise in “levelling up” new markets, not as a way of undermining the standards set in existing markets, especially with MiFID II. This is all the more important in view of **recital 40**,

which indicates that this framework, if deemed successful, could serve as a template for modifying existing EU financial services legislation.

Finance Watch therefore suggests to **delete** the proposed exemption under **Art. 5(4)**. Doing so would not prevent retail investors from using a trading venue under the DLT Pilot, but they would have to do so through an intermediary and under the applicable rules of MiFID II.

4. Role of DLT network nodes (validators)

The performance and, in particular integrity of a DLT infrastructure relies first and foremost on the transparency of its consensus mechanism and the integrity of its validator nodes. This applies to both “permissioned” and “permission-less” DLT infrastructures. Although the proposal is not explicit on this point it appears highly likely that deployments under the DLT Pilot will operate in a “permissioned” mode, i.e. with a limited number of known validator nodes. In the interest of transparency and to ensure compliance with the Anti-Money Laundering Directive (Directive (EU) 2018/1673, AMLD 6), operators of a DLT market infrastructure under the pilot framework should be obliged explicitly to notify the competent authority and/or ESMA, as appropriate, of the identity of the operators of DLT network nodes and, if different, their ultimate beneficial owners (**Art. 6(2) DLT Pilot**).

Operators should also formalise, and disclose, the arrangements between them and members/participants for meeting liabilities to third parties for damages that could arise from a malfunctioning or technical breach of the DLT infrastructure. This information should be updated ad-hoc, as required, and confirmed regularly, at least annually, as part of the reporting obligations under **Art. 9 DLT Pilot**.

5. Relationship with DORA

The proposed regulation on Digital Operational Resilience for the Financial Sector (COM 2020/595 final; DORA) sets out a comprehensive framework for institutions, investment firms and third-party service providers who operate Central Securities Depositories (CSDs) and trading venues are in scope of DORA by virtue of Art. 2(1) DORA. The obligations under DORA should be extended explicitly, for the avoidance of doubt, to operators of DLT network nodes under the DLT Pilot regulation. This could be done by amending **Art. 2(1) DORA** accordingly.

About Finance Watch

Finance Watch is an independently funded public interest association dedicated to making finance work for the good of society. Its mission is to strengthen the voice of society in the reform of financial regulation by conducting advocacy and presenting public interest arguments to lawmakers and the public. Finance Watch's members include consumer groups, housing associations, trade unions, NGOs, financial experts, academics and other civil society groups that collectively represent a large number of European citizens. Finance Watch's founding principles state that finance is essential for society in bringing capital to productive use in a transparent and sustainable manner, but that the legitimate pursuit of private interests by the financial industry should not be conducted to the detriment of society. For further information, see www.finance-watch.org

Finance Watch
Rue Ducale 67 b3
1000 Brussels
T: + 32 (0)2 880 0430

www.finance-watch.org



Finance Watch