McCarthy, Jonathan*

Wrong turns or paths not (yet) taken? The creation of an EU regulatory framework for digital finance

Abstract

This article aims to take stock of the progress made through recent EU legislative initiatives on digital finance, specifically by discerning how the EU has pursued certain options for regulation but has seemingly shirked from addressing some emergent issues. The article describes the influence of the guiding principle of 'same activity, same risks, same rules' in the EU's legislative approach towards digital finance. This article focuses on the Markets in Crypto Assets Regulation (MiCAR) and the Digital Operational Resilience Act (DORA) as the key instances of the EU's legislative efforts to categorise differing 'risks'.

By reference to MiCAR and to DORA, the article highlights the contradiction at the essence of the 'same activity, same risks, same rules' outlook. The article evaluates the potency of MiCAR and DORA in enforcing against activities which are characterised by their elusively shapeshifting traits. The article reflects on the supposedly future-proof qualities of the new EU framework on digital finance by briefly pinpointing some examples of how the legislation remains exposed to changing innovations, which may eventually prompt further reforms to MiCAR and DORA.

Keywords: digital finance; FinTech; crypto-assets; cybersecurity

I. Introduction

For the last decade, financial services have been in the midst of perceptible changes in digitalisation and in the adoption of technological innovations (frequently referred to as 'FinTech'). The European Union has consequently sought to implement an architecture of rules to govern digital finance. At the time of writing, prominent examples of EU legislative intervention have entered into effect, and various aspects of the legislation are being supported by the introduction of regulatory technical

* McCarthy, Jonathan, Lecturer, School of Law, University College Cork, Ireland.

DOI: 10.56749/annales.elteajk.2024.lxiii.4.57

standards. The courage of the EU's approach in striving to confront unprecedented transformations and risks in the provision of modern financial services is not in doubt. However, as expressed in this article, there are persisting questions about the prudence and the likely efficacy of the interventionist stance taken by the EU.

This article aims to take stock of the progress made through the EU legislative initiatives on digital finance, specifically by discerning how the EU has pursued certain options for regulation but has seemingly shirked from addressing some emergent issues. From the outset, the article should acknowledge that it is early to make conclusive judgements as to what could be accomplished by this scale of legislative intervention. In view of the expanding scope of technological developments, it is highly probable that the EU's digital finance regulatory framework will prove capable of adapting to future challenges. The purpose of the article is not, therefore, to represent a dismissively knee-jerk and overly critical response to legislative measures which are currently being brought into force. Yet, it is only by recognising the manifest gaps and shortcomings that future reforms can be appropriately formulated.

The article commences by describing the guiding principle of 'same activity, same risks, same rules', which has sculpted the EU's legislative approach towards digital finance. For all of the ostensible fairness and consistency which is connoted by this principle, the article identifies the flaws of adhering to a 'same activity, same risks, same rules' mindset, particularly in how it inhibits the capacity of regulation to be tailored to emergent problems and legal ambiguities.

The article proceeds to demonstrate h ow the legislative pillars of the EU's framework are oriented towards categorising different forms of risk. By aiming to neatly classify types of risk, the paradox of the 'same activity, same risks, same rules' principle is that, in reality, the legislation is conceding that there are diffuse examples of risks which may require distinct approaches. This article focuses on the Markets in Crypto Assets Regulation (MiCAR)[1] and the Digital Operational Resilience Act (DORA)[2] as the key instances of the EU's legislative efforts to delineate between risks. There are also parallel examples of risk categorisation across other legislative measures which pertain to digital finance.

By reference to MiCAR and to DORA, the article highlights the contradiction at the essence of the 'same activity, same risks, same rules' outlook. The article contends that the original legislative objectives have ironically resulted in an uneven

[1] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937; OJ L 150/40. [hereinafter 'MiCAR']

[2] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011; OJ L 333. [hereinafter 'DORA']

concentration of regulatory attention on particular elements of digital finance and a simultaneous neglect of the observable difficulties and nascent risks associated with other innovations.

The article evaluates the potency of MiCAR and DORA in enforcing the relevant laws against activities which are characterised by their elusively shapeshifting traits. Crypto-asset markets and cyber-threats have been notoriously averse to enforcement from existing regulatory regimes. The regulatory vacuum is ultimately a central motive for the introduction of EU legislative initiatives in respect of crypto-asset markets and operational resilience. However, will these legislative actions stand the test of time by sufficiently mitigating systemic risks in finance for the foreseeable future? Can the legislation avoid being a purely transient bulwark against a selected few risks of contemporary digital finance?

By culminating towards the conclusion, the article will reflect on the supposedly future-proof qualities of the new EU framework on digital finance by briefly pinpointing some examples of how the legislation remains exposed to changing innovations that may eventually prompt further reforms to MiCAR and DORA. The article will consider how a putative application of the 'same activity, same risks, same rules' principle has, all at once, exhibited degrees of bravery, a potentially disproportionate emphasis on discrete facets of finance, possible omissions, and a disregard of the complexities associated with ongoing patterns in crypto-assets and in cyber-risks.

II. Same activity, same risks, same rules

The September 2020 release of the European Commission's Digital Finance Strategy was the catalyst for a package of legislative measures in the interests of "a competitive EU financial sector that gives consumers access to innovative financial products, while ensuring consumer protection and financial stability".[3] The Commission's Strategy declared that the 'same activity, same risks, same rules' principle was to be paid "particular attention to" when addressing new challenges and risks resulting from digital transformation, not least to "safeguard the level playing field between existing financial institutions and new market participants".[4] By using 'same activity, same risks, same rules' as a guiding motif, the Commission affirmed that regulation and supervision should be proportionate by being especially cognisant of the risks of 'significant operators' in financial services. Aside from the introduction of fresh legislation, the preservation of financial stability and the protection of the rights of

[3] See the European Commission website, *Digital Finance Package* (24 September 2020), at: https://finance.ec.europa.eu/publications/digital-finance-package_en (last accessed: 31.12.2024.).

[4] European Commission Communication, *A Digital Finance Strategy for the EU,* COM(2020)591 final, 5.

consumers would be integral when adapting extant conduct and prudential legal rules.[5] Moreover, the Commission committed to a "future proof" legislative framework – built to last by means of regular legislative reviews and interpretative guidance – that "neither prescribes nor prevents the use of particular technologies while also ensuring that regulatory objectives continue to be met".[6]

Aspirational language and terminology can be pervasive in policy-making documents. Nonetheless, academic commentary and scholarship on the regulation of technological innovations is far from being unfamiliar with the logic for all-encompassing endeavours that apply uniform, standardised and rather 'traditional' requirements to novel and emerging practices.[7] The varied complexion of innovations – not just in financial services – can quickly frustrate attempts to utilise a blanket-like legal approach. As understood by Iris Chiu, the growth of financial regulation broadly has occurred through a "patchwork" of different approaches.[8] By critiquing the concept of 'same activity, same risks, same rules', Chiu asserts that the mantra is "prone to excluding nuances and differences in underlying objectives, risk characterisation and proportionality", as well as obscuring regulation "from considering if policy adjustments are needed in the face of innovative developments".[9] Chiu concludes that a functional approach, as epitomised by 'same activity, same risks, same rules', is "potentially vague and insufficient" and lacking in "clear guidance" for regulators.[10]

It is perhaps not entirely revelatory to observe that policy statements may often be easily criticised for their generalised wording or for being bereft of express guidelines. It is even debatable as to whether 'same activity, same risks, same rules' is too constrained. Academics and practitioners may have differing views on whether innovations in digital finance are worthy of specialised techniques of regulation. As articulated by Steven Schwarcz, a fundamental point of disagreement exists as to the level to which FinTech innovations are drastically altering finance, thus justifying the use of completely new forms of regulation.[11] Although there can be uncertainty and occasional scepticism about the true depth of digital transformation, there is a

[5] European Commission Communication, *A Digital Finance Strategy for the EU,* COM(2020)591 final, 15.

[6] European Commission Communication, *A Digital Finance Strategy for the EU,* COM(2020)591 final, 11–12.

[7] For example, see the discussion of 'coherentist' perspectives on the regulation of technologies in R. Brownsword, *Law 3.0: Rules, Regulation, and Technology* (Taylor & Francis, 2020).

[8] I. Chiu, An Institutional Account of Responsiveness in Financial Regulation – Examining the Fallacy and Limits of 'Same Activity, Same Risks, Same Rules' as the Answer to Financial Innovation and Regulatory Arbitrage, (2023) 51 (105868) *Computer Law and Security Review,* 7. DOI: https://doi.org/10.1016/j.clsr.2023.105868

[9] Chiu, An Institutional Account of Responsiveness in Financial Regulation, 9.

[10] Chiu, An Institutional Account of Responsiveness in Financial Regulation, 16.

[11] S. Schwarcz, Regulating Financial Innovation: FinTech, Crypto-Assets, DeFi, and Beyond, (2024) 79 (3) *The Business Lawyer,* 615.

prevailing acceptance among academics that some flexibility – stemming from a principles-based regulatory approach – is essential to striking a balance in carefully regulating for technological advancements in finance.[12] A calibrated principles-based treatment of digital finance could be encouraging of genuinely innovative activities, but, where necessary, enabling the "imposition of appropriate guardrails against risks and negative externalities".[13]

The 'same risks, same activity, same risks' principle is echoed in the wording of the legislation introduced in the aftermath of the Commission's Strategy. MiCAR explicitly corresponds to the 'same activity, same risks, same rules' goal and to the principle of 'technology neutrality'.[14] The aim of applying proportionate rules to myriad kinds of technologies is supported by the objective of lessening regulatory fragmentation through a harmonised EU framework.[15] DORA vindicates its format by stating that an EU Regulation – as opposed to a Directive – should be more effective in reducing regulatory complexity, in fostering supervisory convergence, and in increasing legal certainty, which can accordingly contribute to limiting compliance costs.[16] EU harmonisation is deemed to be warranted in response to legislative disparities and diverse approaches across Member States regarding operational resilience and ICT (information communications technology) security of financial entities.[17] According to DORA's requirements, financial entities should follow "the same approach and the same principle-based rules" when addressing ICT risk, but also take into account "their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations".[18]

The Digital Finance Strategy also led to the enactment of a Regulation for a distributed ledger technology (DLT) pilot regime for securities market operators.[19] Due to the relatively narrower parameters of this Regulation to settlement and post-settlement processes in securities markets, a summary of the DLT pilot regime is beyond the focus of this article.[20] Nonetheless, the 'same activity, same risks, same

[12] See D. Arner, R. Buckley, K. Charamba, A. Sergeev and D. Zetzsche, Governing FinTech 4.0: BigTech, Platform Finance, and Sustainable Development, (2022) 27 (1) *Fordham Journal of Corporate and Financial Law,* 1.
[13] Arner, Buckley, Charamba, Sergeev and Zetzsche, Governing FinTech 4.0, 1., 36.
[14] MiCAR, Recital 9.
[15] MiCAR, Recital 5.
[16] DORA, Recital 14.
[17] DORA, Recital 9.
[18] DORA, Recital 13.
[19] Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU; OJ L 151. [hereinafter 'DLT Pilot Regime Regulation']
[20] See further J. McCarthy, Distributed Ledger Technology and Financial Market Infrastructures: An EU Pilot Regulatory Regime, (2022) 17 (3) *Capital Markets Law Journal,* 288.

rules' ethos is equally evident in the legislative objectives. The DLT Pilot Regime Regulation reinforces its intention to be technologically neutral as regards the use of any particular technology over another[21] – a sentiment which seems somewhat incongruous with how the Regulation is unequivocally providing for a specialised regime for DLT as a specific technology. In addition to 'same activity, same risks, same rules' and technology neutrality, the Regulation is expressly grounded in the need to maintain proportionality and a level playing field for market participants.[22]

As a parallel legislative initiative to the measures provided for by the Digital Finance Package, it should be noted that the EU's Artificial Intelligence Act[23] is similarly informed by the 'same activity, same risks, same rules' principle. The AI Act intends to preclude the fragmented divergence of national rules on AI within the EU market[24] and to nurture a level playing field for operators and market participants.[25] However, in a similar manner to the DLT Pilot Regime Regulation, it could be suggested that this push for a uniform approach is undermined by how the AI Act deliberately categorises AI systems by levels of risk (such as how AI systems' creditworthiness assessments of prospective borrowers in the review of loan applications would be classified as high-risk).[26]

As clarified in the article introduction, the focus of this article is on MiCAR and DORA as the foremost examples of legislation from the Digital Finance Package. For sheer exemplary impact, MiCAR and DORA are ambitiously framed models for other jurisdictions. By grasping the nettle of regulating crypto-asset markets through MiCAR, the EU is placing itself in the position of being a standard-setter internationally.[27] As Matthias Lehmann explains, "[w]hile most countries are still weighing their options or experimenting with the application of existing laws to crypto-assets, the EU has forged ahead with an extremely granular set of rules …".[28] DORA has established rules surrounding the management of cyber-risks, the reporting of incidents, and testing for threats. The regulatory framework that DORA has created

[21] DLT Pilot Regime Regulation, Recital 9.
[22] DLT Pilot Regime Regulation, Recital 10.
[23] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [hereinafter 'AI Act'].
[24] See AI Act, Recital 3.
[25] See AI Act, Recital 82.
[26] AI Act, Annex III.
[27] F. Annunziata, An Overview of the Markets in Crypto-Assets Regulation (MiCAR), (2023) (158) *European Banking Institute Working Paper Series,* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4660379 (last accessed: 31.12.2024.).
[28] M. Lehmann, MiCAR – Gold Standard or Regulatory Poison for the Crypto Industry?, (2024) 61 (3) *Common Market Law Review,* 699, 700.

for financial entities should serve as a case study for other spheres of economic activity and organisations, not just within the EU but internationally. An escalation in cyber-risks, cyber-attacks and threats to cybersecurity is being evinced within EU Member States and internationally.[29]

Both MiCAR and DORA declare that their provisions are anchored to the 'same activity, same risks, same rules' precept. When scrutinising the details of the legislation, it is arguable as to how closely aligned the requirements of MiCAR and DORA are to this motto. As outlined in the next section of the article, MiCAR's definition of crypto-assets is oriented around DLT-type systems and applications. By confining the legislative lens to DLT-based crypto-assets, MiCAR risks wrapping itself in a "regulatory straitjacket" which fails to encompass certain emergent forms of crypto-assets.[30] The initial commentary around MiCAR has found it difficult to separate the legislation from a mood of regulatory apprehension about the prospect of globalised 'stablecoins', or asset-referenced tokens[31] – a categorisation of crypto-assets which will be discussed below. The stringency[32] of MiCAR's rules on asset-referenced tokens weakens the illusion of MiCAR being a wholly proportionate and uniform regime, guided by 'same activity, same risks, same rules'.

For DORA, there are inherent complications in defining a cyber-risk or a cyber-threat. International standard-setting agencies and authorities, such as the Financial Stability Board, have significantly contributed to designing recognised terminology relating to cyber-risks.[33] However, there is a strongly subjective element to definitions of cyber-risks. The absence of a coherently objective definition of a cyber crisis can delay or confuse the implementation of an organisation's crisis management processes.[34] A legal obligation to report incidents and threats is increasingly challenging to practically implement if there is little clarity as to what constitutes a definitive 'incident' or 'threat'.[35] As with MiCAR's categorisations of crypto-assets, the onus is placed on legislation – and accompanying regulatory technical standards – to proffer additional guidance regarding the risks to be managed, reported, and tested for. Otherwise, in sharp contrast to the tenor of 'same activity, same risks, same rules', similar risks will result in diverging internal procedures being followed by financial

[29] ENISA (European Union Agency for Cybersecurity), *ENISA Threat Landscape 2024 (July 2023 to June 2024)* (September 2024).
[30] Lehmann, MiCAR – Gold Standard or Regulatory Poison for the Crypto Industry?, 699, 711.
[31] See Lehmann, MiCAR – Gold Standard or Regulatory Poison for the Crypto Industry?, 699.
[32] See Annunziata, An Overview of the Markets in Crypto-Assets Regulation (MiCAR).
[33] See the FSB Cyber Lexicon (November 2018) at: https://www.fsb.org/2018/11/cyber-lexicon/ (last accessed: 31.12.2024.).
[34] European Systemic Risk Board (ESRB), *Advancing Macroprudential Tools for Cyber Resilience – Operational Policy Tools,* (April 2024), 30.
[35] See generally J. McCarthy, Cyber-Risks in Modern Finance: Building Operational and Regulatory Resilience, (2023) 38 (7) *Journal of International Banking Law and Regulation,* 233.

entities. In sum, an analysis of the substance of MiCAR and DORA casts doubt on whether both initiatives are the most authentic specimens of the 'same activity, same risks, same rules' principle.

III. Everything in its right place: Risk categorisations

1. MiCAR

A shared feature of MiCAR and DORA is the quest for categorisation, principally to differentiate between forms of risk and to allow for varying obligations. In looking to MiCAR, firstly, a cornerstone of the legislation is its classification of separate types of crypto-assets. For the purposes of MiCAR, a 'crypto-asset' is defined as "a digital representation of a value or right that is able to be transferred and stored electronically using distributed ledger technology or similar technology".[36] For the sake of clarity, it should be stressed that – as the title indicates – MiCAR is directed at the markets in issued crypto-assets, rather than trying to be a grand bespoke regime for all legal aspects of crypto-assets. MiCAR is fully applicable to EU Member States from 30 December 2024.

By stipulating that a crypto-asset should have an identifiable issuer in order to fall within the ambit of MiCAR,[37] the legislation does not make provision for 'decentralised' currencies which lack a single point of issuing authority. MiCAR is automatically excluding forms of crypto-based activities which have gained considerable public awareness and media coverage in recent times, especially decentralised finance (DeFi) and non-fungible tokens (NFTs).[38] Even the most famous of decentralised digital currencies, Bitcoin, cannot be adequately captured by the scope of MiCAR. If a crypto-asset platform or provider plans to offer Bitcoin or another pre-existing cryptocurrency – which were admitted to trading before 30 December 2024 – the formalities for offerings (as summarised in the next section) would not have to be complied with until 31 December 2027.[39]

By excluding crypto-assets which are not directly issued by a central offeror, MiCAR's fixation on crypto-asset issuance may hint at an anachronistic perception that most crypto-assets are akin to Initial Coin Offerings (ICOs). In other words,

[36] MiCAR, Article 3(1)(5).
[37] MiCAR, Recital 22.
[38] At a rudimentary level, DeFi involves protocol-based transactions with tokens which may regularly be backed by other digital tokens (stablecoins pegged to fiat money) as security. NFTs are effectively digital representations of owned items, such as photos, videos, music, etc.
[39] MiCAR, Article 143(2)(b).

MiCAR could be fighting the regulatory battles which needed to be fought several years ago in relation to the ICO bubble,[40] rather than comprehending the far more complex and interlinked markets which are now in existence. Even though MiCAR is hamstrung by plainly stating that it cannot regulate for decentralised crypto-based activities, the shortcomings of MiCAR in capturing the steady emergence of DeFi are a blatant omission. DeFi market participants cannot be regarded as crypto-asset service providers under MiCAR, irrespective of how prevalent DeFi activities become within the EU and internationally.[41] As time progresses, the rationale for regulating for DeFi should become more compelling. Linkages between mainstream financial institutions ('traditional' finance) and DeFi platforms may deepen, and, with increased consumer demand for DeFi (thus leading to greater consumer susceptibility to losses from fraud), there may be an increase in demand for regulation.[42]

A contrary perspective would suggest that MiCAR's omission of DeFi can be forgiven. It could be argued that regulators should cautiously look before they leap when regulating for an array of crypto-based activities. Whether it is DeFi, NFTs or commonly known cryptocurrencies like Bitcoin, some commentators adjudge that the 'dress-up clothes' worn by crypto are feeble attempts to play at being genuine financial activity.[43] Much crypto activity continues to be linked to criminal conduct, fraudulent schemes, gambling, and game-like applications.[44]

However, the disputes about categorising what is meant by true 'finance' can merely disclose a fallacy of thinking about financial regulation. As astutely conveyed by Saule Omarova, there can be a 'master narrative' of the financial market as a presumptively socially beneficial mechanism and as an indispensable tool for economic growth. The reality is that private transactions in secondary markets – which are essentially geared towards individualised profit-making – occur at a high frequency and contribute to the development of technological innovations.[45]

---

[40] On the controversies and regulatory difficulties of ICOs, see D. Zetzsche, R. Buckley, D. Arner and L. Föhr, The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators, (2019) 60 (2) *Harvard International Law Journal,* 267, and A. Gurrea-Martínez and N. Remolina León, The Law and Finance of Initial Coin Offerings, in C. Brummer (ed.), *Cryptoassets: Legal, Regulatory, and Monetary Perspectives* (Oxford University Press, 2019).

[41] I. Chiu, The Application of the Markets in Crypto-Asset Regulation to Decentralised Finance, (2023) 38 (12) *Journal of International Banking Law and Regulation,* 432.

[42] See particularly M. Aquilina, J. Frost and A. Schrimpf, Decentralized Finance (DeFi): A Functional Approach, (2024) 10 *Journal of Financial Regulation,* 1.

[43] T. Baker, Let's Stop Treating Crypto as If It Were Finance, (December 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4287185 (last accessed: 31.12.2024.).

[44] For a 2024 snapshot, see Chainalysis, *2024 Crypto Crime Report,* https://go.chainalysis.com/crypto-crime-2024.html (last accessed: 31.12.2024.).

[45] S. Omarova, Financial Innovation: Three Fallacies in the Debate, in S. Omarova, A. Andhov and C. Hill (eds), *Hidden Fallacies in Corporate Law and Financial Regulation. Reframing the Mainstream Narratives* (Bloomsbury Professional, 2025).

MiCAR provides for three categories of crypto-assets: crypto-assets other than asset-referenced tokens or electronic money tokens (as governed by Title II of MiCAR); asset-referenced tokens (including 'significant' asset-referenced tokens) (governed by Title III); and e-money tokens (governed by Title IV). E-money tokens are largely subject to the equivalent rules for e-money by virtue of Directive 2009/110/EC, but the crucial distinction between MiCAR's e-money tokens and e-money generally is that MiCAR-governed tokens are issued on the basis of DLT or a similar cryptographical technology. The 'other' category of crypto-assets, within Title II of MiCAR, archetypally relates to utility tokens which are instrumental to accessing services, software, games, etc. As but one instance of a lacuna which is set to materialise in the years ahead, MiCAR does not ascertain whether NFTs that possess utility functions can still be subsumed within the Title II requirements of the legislation.[46]

MiCAR construes asset-referenced tokens as purporting "to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies".[47] The raison d'être of an asset-referenced token, or stablecoin, is to signify an alternative to the dramatic price volatility of decentralised currencies that are not tied to any real-world reserves of fiat currency. MiCAR's preoccupation with asset-referenced tokens could be attributed to the alarm generated among regulators by the vista of a powerful technological company, or a social media platform, launching its own stablecoin for users.[48] The previous Facebook proposal for a Libra global stablecoin (later re-named Diem) indelibly shaped regulators' attitudes towards the systemic risks presented by large-scale tokenised projects which would be pegged to fiat currency stored with financial institutions and banks.[49]

A global – or even quasi-global – stablecoin arrangement would fit MiCAR's categorisation of a 'significant' asset-referenced token. Chapter 5 of Title III of MiCAR separately classifies significant asset-referenced tokens in accordance with a list of criteria in Article 43. Chapter 2 of Title IV is applicable to significant e-money tokens. As reiterated in the next section, MiCAR expressly curbs the growth of significant tokenised projects by restricting the issuance of asset-referenced tokens

[46] See Annunziata, An Overview of the Markets in Crypto-Assets Regulation (MiCAR), 32.
[47] MiCAR, Article 3(1)(6).
[48] On the context of regulatory fears about the implications of global stablecoin arrangements, see Lehmann, MiCAR – Gold Standard or Regulatory Poison for the Crypto Industry?, 699, 704. For updated recommendations on internationally coordinated responses to global stablecoins, see the FSB's *High-Level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements. Final Report* (July 2023), https://www.fsb.org/2023/07/high-level-recommendations-for-the-regulation-supervision-and-oversight-of-global-stablecoin-arrangements-final-report/ (last accessed: 31.12.2024.).
[49] See E. Nicolle, Ghosts of Facebook's Libra Haunts Stablecoin Rules Five Years Later, *Bloomberg Crypto Newsletter,* (16 April 2024), https://www.bloomberg.com/news/newsletters/2024-04-16/ghost-of-facebook-s-libra-haunts-stablecoin-rules-five-years-later (last accessed: 31.12.2024.).

and e-money tokens that are found to have an estimated quarterly average number of transactions higher than 1 million and an average aggregate value higher than €200,000,000 per day.[50]

The attention devoted towards asset-referenced tokens and stablecoin arrangements erodes the semblance of MiCAR exhibiting an even-handed style in regulating all crypto-assets. Yet, even in MiCAR's provisions on asset-referenced tokens, there are certain omissions. For example, algorithmic stablecoins do not appear to be reined within MiCAR's definition of tokens "referencing another value or right or a combination thereof".[51] Algorithmic stablecoins tend to claim to be able to preserve a stable valuation by use of algorithmic adjustments. To date, algorithmic stablecoins have not lived up to this pioneering promise and have instead garnered public interest due to high-profile collapses of stablecoins such as Terra and Iron Finance.[52]

2. DORA

By comparison with MiCAR, DORA does not set out distinct definitions for types of cyber-risks, threats, or attacks. Nonetheless, DORA does shift responsibility towards financial entities to implement effective frameworks and processes for the management of ICT risks. Fully applicable from 17 January 2025, DORA concentrates on enhancing 'digital operational resilience', as "the ability of a financial entity to build, assure and review its operational integrity and reliability", which can be ensured "either directly or indirectly through the use of services provided by ICT third-party service providers" and which can cover "the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions".[53]

ICT risk management is the focus of Chapter II (Articles 5 to 16) of DORA, whereby financial entities are required to have internal governance and control frameworks for the "prudent and effective" management of ICT risks.[54] An 'ICT risk' is given a wide definition in DORA as "any reasonably identifiable circumstance in relation to the use of network and information systems" which, if materialised, can

[50] MiCAR, Articles 23 and 58(3).
[51] For a similar analysis, see Schwarcz, Regulating Financial Innovation, 615.
[52] For media coverage of the Terra collapse, see A. Chow, The Real Reasons Behind the Crypto Crash, and What We Can Learn from Terra's Fall, *Time,* (17 May 2022), https://time.com/6177567/terra-ust-crash-crypto/ (last accessed: 31.12.2024). For an economic study, see J. Liu, A. Schoar and I. Makarov, Anatomy of a Run: The Terra Luna Crash, (2023) (31160) *National Bureau of Economic Research Working Paper*.
[53] DORA, Article 3(1).
[54] DORA, Article 5(1).

result in the compromise of "the security of the network and information systems, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment".[55] Internal organisational procedures are paramount to risk management, since financial entities' management bodies are given the responsibility for maintaining these frameworks.[56] Updated ICT systems, protocols and tools should be used and maintained by financial entities.[57] To adequately protect ICT systems and to have response measures at the ready, financial entities should continuously monitor and control the security and functioning of systems and tools.[58] Prompt detection of 'anomalous activities' should be facilitated by mechanisms enabled by an entity's incident management process.[59] Crisis communication plans will be required by DORA for the "responsible disclosure of, at least, major ICT-related incidents or vulnerabilities to clients and counterparts as well as to the public, as appropriate".[60]

As will be examined in the next section, in terms of enforcement, the hefty responsibilities of incident reporting and testing for threats are carried by financial entities, rather than by external authorities. Even if DORA allocates burdens towards regulated entities, the layering of obligations should assist in financial entities' construction of the lines of defence, which are vital to an organisation's cybersecurity strategy. As outlined by the ESRB,[61] for financial stability, the first barrier against risks and threats should be financial institutions' detection and defence capabilities. These capabilities can be directly aided by DORA's requirements. From the ESRB's vantage, the second line of defence is a systemic mixture of protections – consisting of standardised practices – and precedes a third line of coordinated action capabilities that have EU-wide applicability and that are instructed by globally accepted guidelines. The second and third barriers may necessitate a higher extent of pan-European collaboration than what is presently afforded through DORA. As elaborated on in the next section, there are proposals and propositions which may be more adept than DORA in significantly bolstering these second and third lines of cyber defence. However, DORA's decisive impact in respect of preliminary detection and defence should not be underestimated, especially through its requirements on third-party risk.

Within Chapter V of DORA (Articles 28 to 44), financial entities are obliged to complete an assessment of 'concentration risk' from their contractual arrangements with third-party service providers.[62] Given that outsourcing is commonplace in

[55] DORA, Article 3(5).
[56] DORA, Article 5(2).
[57] DORA, Article 7.
[58] DORA, Article 9.
[59] DORA, Article 10.
[60] DORA, Article 14.
[61] ESRB, *Advancing Macroprudential Tools for Cyber Resilience.*
[62] DORA, Article 29.

cybersecurity services, a pivotal step taken by DORA is to obligate mandatory contractual provisions in arrangements between financial entities and third-party ICT service providers.[63] Supplementary requirements are provided for in contracts with providers of "critical or important functions".[64] Critical ICT third-party service providers are to be formally designed by European Supervisory Authorities (ESAs) through the auspices of a Joint Committee-established Oversight Forum.[65]

The guidance to be yielded through regulatory technical standards could easily form the basis of several other articles and texts on DORA. For now, the import of DORA's provisions is to show that standardised responses are being expected in relation to cyber-risks. Although it can seem to cleanly conform to the 'same activity, same risks, same rules' stance, the most telling reflection of DORA's fitness for purpose will be in how the risks can actually be combatted through the enforcement of the legislative provisions.

IV. Chasing shadows? The potency of enforcement mechanisms

1. MiCAR

By enacting a dedicated regime for markets in crypto-assets, the EU is pursuing a paradigm of enforcement by prescriptive legislative rules. This differs from an approach of piecemeal sanctions – operating on a case-by-case footing of 'regulation by enforcement'[66] – which has become emblematic of some jurisdictions, such as in the United States through the Securities and Exchange Commission (SEC). Much of MiCAR displays a grafting of standard market rules to the somewhat shadowy realm of crypto-asset issuance. MiCAR's steadfast adherence to existing financial regulatory rules could even instigate accusations of a "copy and paste approach".[67] It remains to be seen whether crypto-asset markets are too shifting or precarious to be the foundations for this transplantation.[68]

When issued crypto-assets – including asset-referenced tokens and e-money tokens – are being offered to the public or are seeking admission to a platform, a white paper must be drawn up and subsequently notified to the relevant competent authority

[63] DORA, Article 30.
[64] DORA, Article 30(3).
[65] DORA, Article 31.
[66] C. Brummer, Disclosure, Dapps and DeFi, (2022) 5 (2) *Stanford Journal of Blockchain Law & Policy,* 137.
[67] Lehmann, MiCAR – Gold Standard or Regulatory Poison for the Crypto Industry?, 699, 707.
[68] See J. McCarthy, Cryptocurrencies. Digital Money and Regulatory Damage, (2022) 37 (8) *Journal of International Banking Law and Regulation,* 282.

of the issuer's home EU Member State.[69] The European Securities and Markets Authority (ESMA) is responsible for maintaining a register of notified crypto-asset white papers. The inclusion of white paper requirements for issued crypto-assets is decidedly a signal of MiCAR's intent to galvanise transparency and disclosure. However, in practice, the force of these requirements may be diluted by the fact that competent authorities' advance approval of a crypto-asset white paper will not be necessary.[70]

MiCAR's inclination towards market rules, which are already known to be reasonably effective in enforcement, is further demonstrated by MiCAR's provisions on the authorisation and operating conditions for crypto-asset service providers and by provisions on the prevention of market abuse. Title V of MiCAR includes obligations for prudential safeguards, based on minimum capital requirements and a quarter of the calculated fixed overheads for the preceding year.[71] As an illustration of MiCAR's interventionist position with regards to the organisational structures of crypto-asset issuers, the legislation provides that the governance arrangements of issuers of asset-referenced tokens and crypto-asset service providers must ensure that members of management "be of sufficiently good repute and possess the appropriate knowledge, skills and experience, both individually and collectively, to perform their duties".[72] The provision specifies that management members must have convictions relating to terrorist financing or money laundering or "any other offences that would affect their good repute".[73] The legislation proceeds to make provision for a requirement capable of rather expansive interpretation that management members "demonstrate that they are capable of committing sufficient time to effectively perform their duties".[74]

MiCAR obliges "adequate arrangements" to be made for the safekeeping of clients' crypto-assets and funds,[75] while crypto-asset service providers must establish and maintain "effective and transparent" procedures for the "prompt, fair and consistent" handling of complaints (in addition to publishing descriptions of the procedures).[76] Crypto-asset service providers must implement and maintain policies to identify, prevent, manage and disclose conflicts of interest.[77]

Title VI of MiCAR extends the imposition of 'normal' market rules by comprising provisions on the prevention and prohibition of market abuse involving crypto-assets. The rules consist of requirements on the public disclosure of inside

[69] MiCAR, Articles 6, 19 and 51.
[70] An insight reiterated in relation to the Commission's initial MiCAR proposal in McCarthy, Cryptocurrencies. Digital Money and Regulatory Damage, 282, 290.
[71] MiCAR, Article 67.
[72] MiCAR, Articles 34(2) and 68(1).
[73] MiCAR, Articles 34(2) and 68(1).
[74] MiCAR, Articles 34(2) and 68(1).
[75] MiCAR, Article 70.
[76] MiCAR, Article 71.
[77] MiCAR, Article 72.

information,[78] the prohibition of insider dealing (arising from the possession and use of insider information),[79] and the prohibition of market manipulation.[80]

Even though Title VII of MiCAR lists a range of powers accorded to competent authorities (including to require provision of information and documents, to suspend, prohibit or order immediate cessation, and to undertake inspections and investigations), it is a matter of conjecture as to how rigorously these powers can be enforced against crypto-asset service providers. The genesis of crypto-assets is rooted in a cyber-libertarian vision of peer-to-peer transactions within decentralised, or 'consensus'-driven, networks.[81] The arrival of a new era of robust EU requirements and obligations could be something of a culture shock for members of the management bodies of crypto-asset issuers.

A plausible by-product of MiCA's implementation is that the EU is about to embark on finding a mini-lateral or regional solution to a globalised phenomenon.[82] As Lehmann argues, the EU could be fastened to a 'Fortress Europe' strategy,[83] buttressed by the armoury of powers that MiCAR gives to competent authorities. A disproportionate weighting of enforcement powers could have the counterproductive result of frightening away crypto-asset service providers from establishing themselves within the EU. Lehmann identifies an apt example of MiCAR's potentially inhibiting effect in the provision for restricting issuance of significant asset-referenced and e-money tokens beyond upper limits on transactions and user numbers. As tersely remarked on by Lehmann, "[o]ne can only surmise how the market is going to react to such a measure. Perhaps it will start enthusiastically about the stablecoin, but then quickly lose interest because of the danger of it becoming "too successful".[84]

The enforcement attributes of MiCAR will be profoundly tested by the absence of clarity on the status of 'financial instruments' and by the failure to bring DeFi satisfactorily within the reach of the legislation. The legislation itself states that MiCAR does not apply to crypto-assets that qualify as financial instruments[85] and which are capable of being traded on securities markets in accordance with Article 4(1)

[78] MiCAR, Article 88.
[79] MiCAR, Article 89.
[80] MiCAR, Article 91.
[81] As most famously encapsulated in the Bitcoin white paper (Bitcoin, *A Peer-to-Peer Electronic Cash System*) of 'Satoshi Nakamoto' (widely reckoned to be a pseudonym), released in 2008; available at: https://bitcoin.org/en/bitcoin-paper (last accessed: 31.12.2024).
[82] On the need to stimulate greater collaboration and coordination between regional blocs, see Y. Yadav, Fintech and International Financial Regulation, (2020) 53 (3) *Vanderbilt Journal of Transnational Law,* 1109.
[83] Lehmann, MiCAR – Gold Standard or Regulatory Poison for the Crypto Industry?, 699.
[84] Lehmann, MiCAR – Gold Standard or Regulatory Poison for the Crypto Industry?, 699, 719.
[85] MiCAR, Article 2(4)(a).

of the second Markets in Financial Instruments Directive (MiFID II).[86] At the time of writing, as per its mandated role in MiCAR,[87] ESMA has released a final report on its guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments.[88] Irrespective of the timing of the issued guidelines being in such close proximity to the date on which MiCAR is due to fully come into force (30 December 2024), it is likely that the courts will retain crucial clout in deciphering whether a crypto-asset can be regarded as a tradeable financial instrument.

As DeFi is, in effect, excluded from the span of MiCA's enforcement powers, there could be legitimate concerns as to how EU regulatory frameworks can address and respond to the risks, vulnerabilities, speculative practices, and fraudulent conduct which are being manifested in DeFi markets. Events over the past two years attest to the innate volatility and interconnectedness of DeFi markets and the broader crypto-asset industry. The much-publicised downfall of the FTX platform and the problems experienced in DeFi platforms were factors in a 'Crypto Winter' from 2022 to 2023, which only further raised calls for more resolute regulatory action.[89] Even though the Commission's MiCAR proposal predated the turmoil of the Crypto Winter, it is difficult to analyse the introduction of MiCAR in isolation from the severe fluctuations and turbulence of DeFi and crypto markets from late 2022 onwards. The fault lines which the Crypto Winter has unveiled are underscoring the benefits of improved cross-border collaboration, including proposals for fresh international standard-setting agencies for digital finance.[90]

If there are paths worth exploring in future amendments to MiCAR, a possibility is to make provision for systems of 'embedded supervision' in DLT- and blockchain-based platforms.[91] As a concept postulated by Raphael Auer, information could be directly at the disposal of regulators that are essentially integrated as network participants in decentralised applications. As prescriptive legislative obligations on

[86] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast); OJ L 173/349.

[87] MiCAR, Article 2(5).

[88] ESMA, *Final Report: Guidelines on the Conditions and Criteria for the Qualification of Crypto-Assets as Financial Instruments* (December 2024) (ESMA75453128700-1323), https://www.esma.europa.eu/document/final-report-guidelines-conditions-and-criteria-qualification-crypto-assets-financial (last accessed: 31.12.2024.).

[89] See particularly D. Arner, D. Zetzsche, R. Buckley and J. Kirkwood, The Financialisation of Crypto: Designing an International Regulatory Consensus, (2024) 53 (105970) *Computer Law & Security Review,* DOI: https://doi.org/10.1016/j.clsr.2024.105970

[90] See the case made for the merits of new global agencies (such as a Digital Stability Board) in Arner, Buckley, Charamba, Sergeev and Zetzsche, Governing FinTech 4.0, 1.

[91] R. Auer, Embedded Supervision: How to Build Regulation into Blockchain Finance, (2019) (811) *Bank for International Settlements Working Paper,* https://www.bis.org/publ/work811.pdf (last accessed: 31.12.2024.).

transparency and disclosure may not always be straightforward to practically enforce, a real-time flow of information through an embedded network would be tantamount to an expedient means for regulators of viewing crypto market activities as they happen.[92] However, it would take time for such an idea to come to fruition. Even if embedded supervision is technically viable, regulators could be criticised for expecting service providers to shoulder the burden of implementing the necessary changes to existing systems.

It could be asserted that a more opportune direction for legislative reforms would be towards the monitoring of social media-generated hype around various crypto-asset offerings.[93] The supply of 'non-formalised' information – and, often, misinformation and disinformation – about crypto-assets can proliferate among 'FinFluencers' on social media. In the minds of prospective users of crypto-asset services, this information can quickly take precedence over any of the details contained in the white papers of crypto-asset issuers. On the other hand, it should be accepted that there are well-documented quandaries in attempting to supervise the dissemination of content on social media platforms. Moreover, as with other enforcement challenges of MiCAR, the potency of the legislation in its current incarnation could be stymied by the pace of developments in crypto-asset markets and the appearance of new kinds of crypto-assets.

2. DORA

Within Chapter III of DORA (Articles 17 to 23), financial entities are required to "define, establish implement" ICT-related incident management processes to "detect, manage and notify" ICT-related incidents.[94] An 'incident' is defined as a "single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity".[95] The processes must have early warning indicators in place,

[92] Regulatory authorities are already becoming accustomed to use of RegTech and SupTech applications in assisting with supervisory functions, as discussed in P. Batista and W. Ringe, Dynamism in Financial Market Regulation: Harnessing Regulatory and Supervisory Technologies, (2021) 4 (2) *Stanford Journal of Blockchain Law & Policy,* 1 and J. McCarthy, The Regulation of RegTech and SupTech in Finance: Ensuring Consistency in Principle and in Practice, (2023) 31 (2) *Journal of Financial Regulation and Compliance,* 186.

[93] A recommendation enunciated in D. Zetzsche, R. Buckley, D. Arner and M. van Ek, *Remaining Regulatory Challenges in Digital Finance and Crypto-Assets After MiCA,* Study for the Committee on Economic and Monetary Affairs (ECON), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament (2023).

[94] DORA, Article 17(1).

[95] DORA, Article 3(8).

have procedures to identify, track, log, categorise, and classify incidents, have roles and responsibilities assigned within the entities, and have plans set out for communications to staff, external stakeholders and media.[96]

Incidents should be classified and their impact determined by reference to criteria, such as: the number and/or relevance of clients or counterparts affected, and, where applicable, the amount or number of transactions affected, and whether the incident has caused reputational damage; the duration of the incident; the geographical spread; data losses (in relation to availability, authenticity, integrity or confidentiality); the criticality of the services affected; and the economic impact.[97] Further guidance has been provided by the ESAs' final report on draft technical standards, submitted to the European Commission in January 2024.[98] However, it should be gleaned from the provisions that the focal decision-making as to what constitutes a notifiable incident will be a matter for the entity itself and its incident management process.

Voluntary notifications of incidents are permitted,[99] but all "major ICT-related incidents" must be reported to the relevant competent authority.[100] A 'major' incident is defined as one which "has a high adverse impact on the network and information systems that support critical or important functions of the financial entity".[101] Financial entities must inform clients "without undue delay" where a major incident occurs and when it impacts clients' financial interests.[102]

DORA sets a course for an assessment of how to centralise major incident reporting, specifically through a single EU hub.[103] A joint ESAs report is to "explore ways to facilitate the flow of ICT-related incident reporting, reduce associated costs and underpin thematic analyses with a view to enhancing supervisory convergence".[104] The provision is envisaging a necessary step towards the coordination of incident reporting. The obvious impediment to a smoothly designed central locus of incident reports is that a hub could become overloaded with submitted notifications from entities. Reporting overload could be especially prompted if the meaning of a major incident – as a subjective evaluation by an entity under its own risk management processes – is clouded in ambiguities. Furthermore, while the detection and reporting of incidents may show DORA's appreciation of the necessity for emergency responses, DORA is not advancing

[96] DORA, Article 17(3).
[97] DORA, Article 18(1).
[98] ESAs, *Final Report on Draft Regulatory Technical Standards specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554* (January 2024) (JC 2023 83).
[99] DORA, Article 19(2).
[100] DORA, Article 19(1).
[101] DORA, Article 3(10).
[102] DORA, Article 19(3).
[103] DORA, Article 21.
[104] DORA, Article 21(1).

solutions to tackle the potentially systemic repercussions of a major cyber incident and crisis affecting a gamut of financial entities across the EU.

By narrowly charting a route towards strengthening financial entities' standards of operational resilience, DORA may have overlooked the merits of joining its provisions with the work of current cross-sectoral collaborative networks, such as EU-CyCLONe. EU-CyCLONe is a cooperation arrangement between the national authorities of EU Member States for the management of cyber crises. Since its informal creation in 2020, EU-CyCLONe is now a fully-fledged liaison network, legally recognised through the second Network and Information Security (NIS) Directive.[105] A foremost aspect of EU-CyCLONe's activities is engagement in preparing cross-border incident reporting mechanisms and crisis response planning. In a financial context, as a complementary layer of coordination of incident reporting to DORA, the ESRB has recommended the establishment of a pan-European systemic cyber incident coordination framework (EU-SCICF). EU-SCICF is proposed to enable designated points of contact for the ESAs, the European Central Bank (ECB) and the competent authorities within each EU Member State.[106]

Within Chapter IV of DORA (Articles 24 to 27), financial entities are expected to "establish, maintain, and review a sound and comprehensive" testing programme for "the purpose of assessing preparedness for handling ICT-related incidents, of identifying weaknesses, deficiencies and gaps in digital operational resilience, and of promptly implementing corrective measures".[107] Certain types of tests are specified in the legislation, such as vulnerability assessments and scans, open source analyses, scenario-based testing, performance testing, and penetration testing.[108] By prescribing some tests as being more appropriate than others, it could be queried whether DORA is showing itself to be capable of adjusting to future refinements in testing techniques.[109]

With exceptions,[110] financial entities must carry out advanced threat-led penetration testing at least every three years, but competent national authorities may

[105] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive); OJ L 333/80.

[106] Recommendation of the ESRB of 2 December 2021 on a pan-European systemic cyber incident coordination framework for relevant authorities (ESRB/2021/17). For a summary of the proposal, see also ESRB, *Advancing Macroprudential Tools for Cyber Resilience,* Box 3, 31.

[107] DORA, Article 24(1). Article 24(4) stipulates that testing should be undertaken by independent parties, "whether internal or external".

[108] DORA, Article 25(1).

[109] McCarthy, Cyber-Risks in Modern Finance, 233, 238.

[110] Microenterprises are excluded from this requirement, but Article 16 of DORA also provides for exclusions for small and non-interconnected investment firms, payment institutions and e-money institutions who are exempt through the second Payment Services Directive (Directive (EU) 2015/2366) and the second e-Money Directive (Directive 2009/110/EC), exempted institutions

request reductions or increases in this frequency of testing.[111] Threat-led penetration testing must "cover several or all critical or important functions of a financial entity" and be performed "on live production systems supporting such functions".[112] DORA's standards for threat-led penetration testing are to be devised in accordance with the TIBER-EU (Framework for Threat Intelligence-based Ethical Red Teaming) procedures for testing.[113] Team-centred simulation exercises, or 'war games', of conducting test threats and attacks on cyber defences are fundamental testing methods in modern cybersecurity practices. However, as with numerous measures in the digital finance legislation, the winds of change are beginning to be felt in cybersecurity. As contemplated in the final section, MiCAR and DORA will be judged for their ability to withstand and adapt to these changes.

V. Future-proofed? Or shaped by the next gust of innovations?

In light of the avowed aim of the Commission's 2020 Digital Finance Strategy to implement a "future-proof" legislative framework, this article's evaluation of the current state of EU digital finance regulation concludes by reflecting on some salient features which may be especially affected by future developments.

MiCAR marks a bold progression of the EU's treatment of crypto-assets. Regardless of whether the intervention can be viewed as being hasty or overdue, there are omissions to the scope of MiCAR. As recognised in the preceding sections, MiCAR could fall behind an impetus of market developments in DeFi, crypto lending and staking, and tokenisation. For commentators such as Lehmann, MiCAR is simply not future-proofed, and an updated 'MiCAR 2.0' should be reasonably anticipated.[114] Aside from the threat of MiCAR beginning to prematurely show its vintage and being out of touch with crypto-asset innovations, there could be ramifications for present-day crypto activities within EU Member States. If MiCAR can, in retrospect, be seen as an "overly zealous" interference in crypto-asset markets, the EU's standing within the global crypto landscape could be diminished.[115] Other jurisdictions may take a comparably more lenient view of crypto activities and take a more supportive line

through the Credit Institutions Directive (Directive 2013/36/EU), and small institutions which make provision for occupational retirement.

111 DORA, Article 26(1).

112 DORA, Article 26(2).

113 See ECB, *TIBER-EU Framework. How to Implement the European Framework for Threat Intelligence-based Ethical Red Teaming* (May 2018).

114 Lehmann, MiCAR – Gold Standard or Regulatory Poison for the Crypto Industry?, 699, 710.

115 Lehmann, MiCAR – Gold Standard or Regulatory Poison for the Crypto Industry?, 699, 700.

towards ventures such as stablecoin/asset-referenced token projects. The number of crypto-asset issuers who choose to establish within the EU could thereby be limited.

Tokenisation carries significant promise in transforming the efficiency of core components of financial services. There are 'legitimate' or antiquated functions of finance – as epitomised by the older antecedents of ledger recording – to which modern innovations can be applied. The rate of adoption of tokenised methods within 'traditional' areas of financial practice remains negligible. There are unresolved concerns over the practical feasibility of DLT tokenisation, including market demand, interoperability hurdles, suitability for multiple transactions, and questions as to the applicable legal and regulatory frameworks.[116] Tokenisation and DLT have become engulfed in connotations of crypto-assets, stablecoins, cryptocurrencies and DeFi. Yet, clearing and settlement processes could be radically accelerated and made more cost-effective by the 'atomic' qualities of DLT-based tokenised systems.[117] The evolution of tokenisation can also dovetail with the ongoing plans for the imminent launch of a digital euro, as an ECB digital currency, whereby tokenised platforms may be trialled for the digital euro.[118] A burgeoning of efficient EU financial services could be harmed if MiCAR has the unintended effect of stifling the growth and credibility of tokenisation. An EU-centric regulatory mentality could also be overtaken by a prevailing momentum towards relatively more conducive regulatory approaches towards tokenisation, as exemplified by the potential policies of the Trump presidency in the United States.[119]

The environmental consequences of the intensified digitalisation of financial services have already become a policy dilemma. The energy consumption of blockchain technologies, AI, and advanced data analytics poses a stark question as to how regulatory frameworks can seek to actively promote innovative technologies, while still claiming to be acting with environmentally beneficial and sustainable practices to the fore. Under MiCAR, the white papers of the issuers of crypto-asset tokens, asset-referenced tokens and e-money tokens must contain information "on the principal

[116] See further FSB, *The Financial Stability Implications of Tokenisation* (October 2024).

[117] Bank for International Settlements and Committee on Payments and Market Infrastructures, *Joint Report to G20: Tokenisation in the Context of Money and Other Assets: Concepts and Implications for Central Banks* (October 2024).

[118] See the ECB digital euro website at: https://www.ecb.europa.eu/euro/digital_euro/html/index.en.html (last accessed: 31.12.2024.); ECB, *Second Progress Report on the Preparation Phase of a Digital Euro* (2024); and European Commission, Proposal for a Regulation of the European Parliament and of the Council on the Establishment of the Digital Euro, COM(2023)369 final.

[119] See B. Munster, Trump's Courting of the Crypto Industry Could Spell Trouble for Europe, *Politico,* (24 July 2024), https://www.politico.eu/article/donald-trump-courting-technology-crypto-industry-alarm-europe/ (last accessed: 31.12.2024.). For academic commentary on the direct involvement of the Trump family in DeFi tokenisation, see D. Krause, The Risks of the Trump-Backed WLFI Governance Token, *Oxford Business Law Blog,* (17 December 2024), https://blogs.law.ox.ac.uk/oblb/blog-post/2024/12/risks-trump-backed-wlfi-governance-token (last accessed: 31.12.2024.).

adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanism used".[120] The inclusion of this requirement was moderately welcomed as an indication of the legislation's cognisance of environmental factors, albeit opined to be a requirement which could have gone further.[121] As the energy costs of the blockchain/DLT and AI efflorescence continue to mushroom,[122] more restrictive and detailed rules on reporting and on limiting environmentally detrimental expenses should be considered for addition to MiCAR, sooner rather than later.

Like MiCAR, DORA went to great lengths to introduce a series of requirements, notably for financial entities' risk management, incident reporting and testing. As with MiCA, DORA has valiantly gone about creating a sophisticated apparatus of risk detection structures for EU financial services in the interests of operational resilience. The importance of this legislative endeavour should not be discounted. In all probability, similar standards will incrementally be brought to bear on other spheres of economic activity, beyond finance, by following the DORA example. However, the net effect of DORA's requirements is to place a sizeable burden on financial entities to comply with the legislation by implementing risk management processes, determining the internal organisational procedures for incident reporting, and conducting advanced testing.

When the onus is on financial entities to make the necessary overhaul for legislative compliance, it should be realised that suitably rigorous cybersecurity will hinge on the ability of financial entities to pay the costs and to hire qualified staff. As appraised by the ESRB, keeping pace with evolving cyber risks and threats will demand additional investment "to build cyber expertise and capability".[123] Increased resources and skilled personnel are inevitably centrifugal to strengthening cybersecurity and operational resilience. Only time will reveal what the side effects of the rise in compliance requirements will be for EU-based financial entities.

As financial entities cope with the practicalities of compliance and make budgetary adjustments, there are experimental possibilities for financial institutions that are already adopting a new generation of AI and machine learning systems. Generative AI has the capabilities to be used in operational resilience contexts. By processing vast volumes of data, generative AI and other AI models can be directed towards detecting risks and

[120] MiCAR, Article 6(1)(j), Article 19(1)(h), and Article 51(1)(g).

[121] M. Demertzis, Is MiCA the End of the Crypto Wild West? (Bruegel, 5 July 2022), https://www.bruegel.org/comment/mica-end-crypto-wild-west (last accessed: 31.12.2024.).

[122] For example, see E. Kolbert, The Obscene Energy Demands of AI, *The New Yorker,* (9 March 2024), https://www.newyorker.com/news/daily-comment/the-obscene-energy-demands-of-ai (last accessed: 31.12.2024.). For a more optimistic perspective on the future energy consumption costs, see T. Papandreou, Who Wins the Energy Race: AI Data Centers, EVs, or Bitcoin Mining? *Forbes,* (30 August 2024), https://www.forbes.com/sites/timothypapandreou/2024/08/30/who-wins-the-energy-race-ai-data-centers-evs-or-bitcoin-mining/ (last accessed: 31.12.2024.).

[123] ESRB, *Advancing Macroprudential Tools for Cyber Resilience,* 39.

vulnerabilities.[124] Progress will relentlessly be made towards AI systems acting more autonomously as 'agents', rather than 'tools' per se, particularly in facilitating incident reporting and testing.[125] Team testing could occur through AI agents, rather than having humans participating in simulations of cyber threats against ICT systems. Much-vaunted predictions of a 'superintelligence' future of AI advancements are not only captivating for the imagination of the general public.[126] The predictions about how AI could conceivably infiltrate a variety of aspects of financial services can be grounded in relatively logical estimates. Against a backdrop of spiralling investment into laboratory research of AI technologies – even when widespread adoption of AI is only nascent or gradual – the stakes are getting higher in terms of ever more advanced outcomes.

EU regulators will therefore have to be alert to the need for DORA – and MiCAR – to cross-refer and link to parallel legislative initiatives on AI. For example, this may entail specialised DORA provisions on the use of AI in threat-led testing, which explicitly refer to corresponding provisions in the AI Act. In future, the task may not be so much as to future-proof digital finance legislative frameworks as detached units, but instead to cohesively knit together a fabric of EU legislation to weather impending changes and innovations.

VI. Conclusion

This article has portrayed the creation of the EU's regulatory framework on digital finance by reference to its origins in the 'same activity, same risks, same rules' principle. By specifically focusing on MiCAR and DORA, the article argues that the principle is not as consistently formative to the legislation as the Commission initially proclaimed. MiCAR and DORA are oriented around risk categorisations, whether it be in the classification of types of crypto-asset tokens or in the definitions of ICT risks to be addressed within financial entities' management processes. The article identified how both examples of legislation opt to concentrate on requirements relating to certain risk categories, even though there are patent omissions to the scope of the legislative frameworks in view of contemporary developments in crypto-asset markets and

[124] J. Crisanto, C. Benson Leuterio, J. Prenio and J. Yong, Regulating AI in the Financial Sector: Recent Developments and Main Challenges, (2024) (63) *Bank for International Settlements – Financial Stability Institute Insight on Policy Implementation,* https://www.bis.org/fsi/publ/insights63.pdf (last accessed: 31.12.2024.).

[125] See I. Aldasoro, S. Doerr, L. Gambacorta, S. Notra, T. Oliviero and D. Whyte, Generative Artificial Intelligence and Cyber Security in Central Banking, (2024) (145) *Bank for International Settlements,* https://www.bis.org/publ/bppdf/bispap145.pdf (last accessed: 31.12.2024.).

[126] See L. Aschenbrenner, *Situational Awareness. The Decade Ahead,* (June 2024), https://situational-awareness.ai/ (last accessed: 31.12.2024.).

cybersecurity. Put simply, the 'same activity, same risks, same rules' adage is not readily evident from the finished products of MiCAR and DORA.

The article considered the undoubted enforcement challenges faced by MiCAR and DORA. Crypto-asset markets and cyber risks are almost defined by their very elusiveness and tendency to be averse to, or immune from, existing regulatory regimes. Although the requirements of MiCAR and DORA were synopsised, the article pointed towards the limitations and deficiencies of the legislative measures in vociferously enforcing their provisions against modern patterns in crypto-asset usage and in cybersecurity threats. The article progressed to briefly reflecting on how well the legislation is 'future-proofed' against ongoing changes in technologies. The candid conclusion must be that MiCAR and DORA will have to be versatile in being reconfigured towards continuing and emerging issues and innovations. To symmetrically repeat a statement in the article's introduction, the article does not eagerly spring to an undue criticism of the legislative initiatives, but rather, has openly admitted the flaws and the room for augmenting the present requirements of MiCAR and DORA.

This article's title may give the impression that the EU has made clear-cut and dichotomous choices in regulating for digital finance, but the regulatory picture is more nuanced than that. It would be altogether too harsh to intimate that 'wrong' approaches were taken. The legislative intervention has shown how ambitious and intrepid the EU is in responding to regulatory problems in digital finance. There are omissions. There are also paths which can still be taken – and which, as contended in this article, must be taken in future. Wide-ranging, laden with intricacies, and with gruelling phases of implementation and technical standards, the legislative road which has been taken thus far can only be good enough for now.