

DIGITAL OPERATIONAL RESILIENCE IN CRYPTO AND DECENTRALISED FINANCE

JANNIK WOXHOLTH* & DIRK A. ZETZSCHE**

Several regulators have taken steps to strengthen operational resilience of crypto and Decentralised Finance (“DeFi”) systems. We inquire into the effectiveness of such policy approaches against the background of the EU’s Digital Operational Resilience Act (“DORA”). To further legitimate cybersecurity and national security concerns, DORA relies on a risk management pyramid with financial institutions at the top and ICT service providers below. Using DeFi lending and internationally launched stablecoins as examples, we show that both centralised crypto and DeFi systems are rooted in cooperation and decentralisation. By mandating hierarchical risk management in its pursuit of resilience, DORA-style legislation undermines crypto’s ambition of achieving the same goal through horizontal financial infrastructures, potentially sacrificing groundbreaking innovations for incremental gains. Taking the EU Markets in Crypto-assets Regulation (“MiCA”) as a regulatory blueprint, we reconcile the policy paradigms of DORA and crypto and propose policy steps that ensure cyber resilience in crypto networks.

I. INTRODUCTION

Since stone tools, technology has been a driving force throughout human history. Irrigation, weapons and writing technologies shaped early civilisations, and the more innovative and adaptive ones have consistently conquered and outcompeted their rivals for millennia. Rulers have always sought to regulate the power of technology, from the ancient monopolisation of bronze, chariots and catapults, through Chinese and later European gunpowder monopolies, to modern-day nuclear, computer chip or artificial intelligence (“AI”) regulation.¹ Paradoxically, the act of controlling innovation also holds it back, pitting short-term stability against long-term progress.

* PhD; Former Senior Research Scientist; ADA Chair in Financial Law (Inclusive Finance), University of Luxembourg.

** Professor of Law, Dr iur., Dr iur. habil., LL.M.; ADA Chair in Financial Law (Inclusive Finance); Co-coordinator, Centre for Sustainable Governance and Markets, University of Luxembourg; Co-lead, FinTech National Centre of Excellence in Research; Co-chair, Fintech Working Group, European Banking Institute, Frankfurt.

This research was funded in whole, or in part, by the Luxembourg National Research Fund (FNR), grant reference NCER22/IS/16570468/NCER-FT.

¹ See eg, John F Guilmartin, “Military Technology”, *Encyclopaedia Britannica* <<https://www.britannica.com/technology/military-technology>> (26 July 1999).

This tension is evident in two developments that have recently gained momentum in financial regulation. The first is the regulation of cyber resilience² based on a top-down risk management approach.³ This approach aims to safeguard financial stability and national security. A prominent example is the EU Digital Operational Resilience Act (“DORA”).⁴ It was partly preceded and followed by similar initiatives in other countries.⁵ The second is the crypto industry, which features a duality of more centralised set-ups (Crypto CeFi) and more decentralised set-ups (DeFi).

We inquire in this article into the effectiveness of regulatory approaches where these two trajectories intersect. Such an analysis is justified for several reasons. One is that crypto-assets reached a peak value of US\$4 trillion in October 2025.⁶ Another is that Bitcoin is becoming part of the strategic reserves of several countries⁷ and a third is the global race for stablecoin dominance.⁸ Beyond these economic and geopolitical factors, there are important doctrinal implications. Crypto is increasingly regulated globally. The EU Markets in Crypto-assets Regulation (“MiCA”)⁹ is a frontrunner. Other jurisdictions, including Singapore,¹⁰ the UK¹¹ and the US,¹² are developing their own approaches, often with one eye on MiCA. The collision of hierarchical legal approaches, as seen in DORA, and decentralised crypto set-ups raises foundational questions of law. These questions should be addressed for an

² We use the term “cyber resilience” as equivalent to “digital operational resilience” as defined in Digital Operational Resilience Act, EU Parliament and Council Regulation 2022/2554 at 25, [2022] OJ L 333/1 at Art 3(1), <<https://eur-lex.europa.eu/eli/reg/2022/2554>> (accessed 18 July 2026) [DORA].

³ *Ibid* at (10)–(13). On the background of DORA, see D.A. Zetsche and J Woxholth, *The EU Law on Crypto-Assets: A Guide to European FinTech Regulation* (Cambridge: CUP, 2025) 246–249 [Zetsche and Woxholth].

⁴ DORA; Digital Operational Resilience for the Financial Sector, EU Parliament and Council Directive 2022/2556, [2022] OJ L 333/153, <<https://eur-lex.europa.eu/eli/dir/2022/2556/oj/eng>> (accessed 18 July 2026). In line with common usage, the term “DORA” is used in the following both as a reference to the Regulation specifically and the overall DORA framework comprising the Regulation, the Directive, and accompanying L2 legislation. For reasons of brevity, we forego references to L2 legislation unless strictly necessary. For a full overview, see European Commission, “DORA - Implementing and delegated acts: full list”, <https://finance.ec.europa.eu/document/download/7a2d42d8-4b48-4e2e-9b4c-c4e9107686d1_en?filename=dora-level-2-measures-full_en.pdf> (2 July 2025).

⁵ For instance, in the areas of incident reporting and internet of things (“IoT”) devices. See E Fahey, “The Evolution of EU-US Cybersecurity Law and Policy: on Drivers of Convergence” (2024) 46(7) J Eur Integration 1073 at 1078–1081.

⁶ Coingecko, “Global Cryptocurrency Market Cap Charts” <<https://www.coingecko.com/en/charts>>.

⁷ Florian Wimmer, “Bitcoin Strategic Reserves – What They are and Why They Matter”, *Blockpit* <<https://www.blockpit.io/blog/bitcoin-strategic-reserves>> (8 April 2026).

⁸ See Hung Tran and Barbara C Matthews, “The Stablecoin Race”, *Atlantic Council* <<https://www.atlanticcouncil.org/blogs/econographics/the-stablecoin-race>> (10 July 2025).

⁹ Markets in Crypto-assets Regulation, EU Parliament and Council Regulation 2023/1114, [2023] OJ L 150/40, <<https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng>> (accessed 18 July 2026) [MiCA].

¹⁰ Emerging gradually under new and existing acts. See eg, Monetary Authority of Singapore, “MAS Clarifies Regulatory Regime for Digital Token Service Providers” <<https://www.mas.gov.sg/news/media-releases/2025/mas-clarifies-regulatory-regime-for-digital-token-service-providers>> (6 June 2026).

¹¹ Financial Services and Markets Act 2000 (Regulated Activities and Miscellaneous Provisions) (Cryptoassets) Regulations 2025 (SI [draft] 2025 No 000) (UK).

¹² Guiding and Establishing National Innovation for US Stablecoins Act 12 USC §§ 5901–5916 (2025); Digital Asset Market Clarity Act of 2025, HR 3633, 119th Cong (2025) [draft].

effective regulatory response to crypto, ensuring a sound balance between financial stability, national security and openness to innovation.

In the remainder of this article, the term “DeFi” serves, somewhat inaccurately but nevertheless purposefully, as a collective term for both the CeFi and DeFi set-ups of crypto, *ie*, for crypto in general. With this terminology, we not only follow leading articles on crypto but also hint at the commonalities of all crypto set-ups, whether CeFi, DeFi or something in between.¹³ These are blockchain-enabled peer-to-peer services and horizontal networks vested in the cooperation of many independent servers (nodes) that seek to replace the trust we place in financial institutions.¹⁴ To justify this terminology, however, we will first demonstrate why both the more centralised and the more decentralised crypto set-ups face similar challenges regarding the hierarchical risk management embedded in DORA and similar approaches that have emerged globally.

Given the relative novelty of regulation on both cyber resilience and DeFi, we refer to the emerging literature on DORA as a legal concept while our focus is on the intersection with DeFi, which, to our knowledge, has not received any academic attention to date.¹⁵

¹³ On DeFi, see Fabian Schär, “Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets” (2021) 103 2 Federal Reserve Bank of St Louis Review 153 [Schär]; Dirk A Zetzsche, Douglas W Arner, and Ross P Buckley, “Decentralized Finance” (2020) 6(2) Journal of Financial Regulation 172 [Zetzsche, Arner and Buckley].

¹⁴ Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, *Bitcoin.org* <<https://bitcoin.org/bitcoin.pdf>> (21 August 2008) (arguing that blockchains could prevent illicit meddling in financial data) [Nakamoto].

¹⁵ See Eyup Kun, “Challenges in Regulating Cloud Service Providers in EU Financial Regulation: From Operational to Systemic Risks, and Examining Challenges of the New Oversight Regime for Critical Cloud Service Providers under the Digital Operational Resilience Act” (2024) 52 Computer L & Sec Report at 105931 (challenging DORA’s overlapping oversight regime for cloud service providers) [Kun]; Christopher P Buttigieg and Beatriz Brunelli Zimmermann, “The Digital Operational Resilience Act: Challenges and Some Reflections on the Adequacy of Europe’s Architecture for Financial Supervision” (2024) 25 ERA Forum 11 (pointing to challenges in supervisory convergence and proposing a more centralised supervisory architecture); Andrew Pattison, *DORA: A Guide to the EU Digital Operational Resilience Act* (Ely: IT Governance Publishing, 2024); Jonathan McCarthy, “Cyber-Risks in Modern Finance: Building Operational and Regulatory Resilience” (2023) 38 7 J Intl Banking L & Reg 233; Anita Neumannová *et al*, “The Digital Operational Resilience Act for Financial Services: A Comparative Gap Analysis and Literature Review”, in *Information Systems* Maria Papadaki *et al* ed(s) (Springer, Cham, 2023) 570; Daniel Morgan, “Coming to Terms with DORA” (2023) 8 Computer Fraud & Security; Thorsten Ammann *et al*, “Exploring Operational Resilience in Financial Services – the Effects of DORA on Risk and Regulation in Top 3 Financial Markets” (2023) 24 2 Computer Law Review International; Paul Voigt and Verena Ritter-Döring, “Der Digital Operational Resilience Act” (2023) 39 2 Computer & R, CR 82; Rois Ni Thuama and Sean S Costigan “DORA – Understanding the New Regulatory Framework on Digital Operational Resilience” (2023), available at SSRN, <http://dx.doi.org/10.2139/ssrn.4549564>; Khanim Avsuvorova, “Navigating Digital Transformation: Unpacking the Impact of DORA on the Insurance Landscape” (2023), available at SSRN, <http://dx.doi.org/10.2139/ssrn.4549704>; Katarzyna Parchimowicz, “Do Not Get Lost in the Cloud. How EU Financial Institutions Could Avoid Legal and Practical Problems with Cloud Services Arising under DORA” (2023), available at SSRN, <http://dx.doi.org/10.2139/ssrn.4486264>; Hal S Scott, “The E.U.’s Digital Operational Resilience Act: Cloud Services & Financial Companies” (2021) <<https://www.pifinternational.org/wp-content/uploads/2022/08/The-E.U.s-Digital-Operational-Act-Cloud-Services-Financial-Companies-08.06.2021.pdf>> (12 August 2021) [Scott]; Narasimha Rao Aluguju, “Digital Operational Resilience Act (DORA)” (2024) 15 6 International Journal of Computer Engineering and Technology 911.

This intersection highlights the core regulatory challenge of balancing resilience with innovation, which DORA purports to address.¹⁶ We will argue, however, that DORA was not designed with DeFi in mind. By including crypto service providers and issuers within its scope of application, DORA adopts a hierarchical approach to an industry predicated on cooperation and decentralisation.

Small but interdependent actors will struggle to bear the regulatory burden of protecting the crypto system at large against cyber threats. However, even where large actors exist, as in the case of stablecoins with global reach, issued by the likes of Tether and Circle, DORA's approach often results in impossible demands, as the chain of command that DORA anticipates is rarely present in crypto. In turn, regulators stand at a crossroads. They face several unfortunate, if not outright unrealistic, pathways forward. Options include prohibiting crypto due to its non-compliance with DORA, under-enforcing DORA or relying entirely on crypto technology providers with expertise from fields other than financial regulation instead of the financial institutions that DORA assigns to be in charge.¹⁷ In the remainder of the article, we seek to develop a balanced approach between these extremes.

Part II introduces the policy challenge of regulating innovation in the cyber domain, and Part III analyses DORA and its impact on centralised and decentralised crypto set-ups, arguing that the collision of DORA and crypto leads to undesirable outcomes; Part IV presents policy considerations and Part V concludes.

II. CYBER RESILIENCE VERSUS INNOVATION

How to regulate innovation is widely discussed in the field of financial technology ("FinTech") regulation.¹⁸ However, the intersection with cyber resilience adds a new layer of complexity.

A. *Cyber Resilience as Regulatory and DeFi Paradigm*

What is true in the analogue world is true in the digital environment. Value, in whatever form, is exposed to the risk of theft, fraud and technical malfunctions, initiated by both private and state-sponsored perpetrators. Finance is the second

¹⁶ DORA originates from the 2018 "FinTech Action Plan: For a More Competitive and Innovative European Financial Sector". See DORA at (6) and European Commission, Proposal for Regulation on Digital Operational Resilience, [2020], <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020PC0595>> (accessed 18 July 2026).

¹⁷ For instance, the NIS2 Directive seeks to ensure cyber resilience irrespective of financial institutions. See on NIS2, Niels Vandezande, "Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor" (2024) 52 Computer L & Sec Report 105890.

¹⁸ See eg, Christopher Ruof, *Regulating Financial Innovation* (Princeton: Springer, 2023); Hilary J Allen, "Experimental Strategies for Regulating Fintech" (2020) 3 1 Journal of Law & Innovation 1; Dirk A Zetsche, Ross P Buckley, Janos N Barberis and Douglas W Arner, "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation" (2017) 23 1 Fordham J Corp & Fin L 31; Chris Brummer and Yesha Yadav, "FinTech and the Innovation Trilemma" (2019) 107 Geo LJ 235.

most exposed industry to cyber-attacks,¹⁹ and finance CEOs rank cybersecurity among their top concerns.²⁰

In response, the world's regulators are focusing on enhancing the robustness of their cyber resilience frameworks for finance.²¹ A number of international standard-setting bodies and industry self-regulation initiatives have reflected on the borderless nature of the problem.²² They have also raised concerns about duplicated compliance burdens across jurisdictions.²³ For instance, the International Organization of Securities Commissions ("IOSCO") urges its members "to continue to draw from existing, prominent cyber frameworks developed by experts in this field".²⁴

At the same time, the crypto industry is developing its own, primarily technical, solutions to the cyber resilience challenge. Originating from a mistrust in centralised government and financial institutions, distributed ledger technology ("DLT") was created to establish an alternative peer-to-peer financial system governed by consensus among nodes in a distributed network.²⁵ This reduces the likelihood of a single point of failure, offering the promise of new and fundamentally better ways of tackling the cybersecurity challenge in finance.²⁶ Like other emerging technologies, however, DeFi carries its own risks. DeFi platforms are not as distributed²⁷ and the algorithms are not as robust as many believe.²⁸ This leaves them open to so-called "governance attacks" which exploit the governance mechanisms in DeFi protocols.²⁹ As financial data are often generated by just two entities, the buyer and

¹⁹ IBM, "X-Force Threat Intelligence Index", <<https://www.ibm.com/reports/threat-intelligence>>.

²⁰ KPMG, "KPMG 2024 Banking CEO Outlook", <<https://assets.kpmg.com/content/dam/kpmgsites/xx/pdf/2024/10/ceo-outlook-banking-report.pdf>>.

²¹ Financial Stability Institute, "'Banks' Cyber Security – a Second Generation of Regulatory Approaches", <<https://www.bis.org/fsi/publ/insights50.htm>> (12 June 2023) [Financial Stability Institute]. While Hong Kong and Singapore were early movers, the US now follows Europe in addressing the harmonisation of its regulatory framework. See Congressional Research Service, "Introduction to Financial Services: Financial Cybersecurity" <<https://crsreports.congress.gov/product/pdf/IF/IF11717>> (1 May 2023).

²² See *eg*, Bank for International Settlements, "Principles for Operational Resilience" <<https://www.bis.org/bcbis/publ/d516.pdf>> (31 March 2021); Bank for International Settlements, "Revision to the Principles for the Sound Management of Operational Risk" (31 March 2021); Bank for International Settlements, "Principles for the Sound Management of Third-Party Risk" (9 July 2024). For a review of key standards, see The International Organization of Securities Commissions, "Cyber Task Force Final Report" <<https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf>> (June 2019) [IOSCO].

²³ See Anton N Didenko, "Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonization in the European Union and Beyond" (2020) 25 *1 Unif L Rev* 125 at 148–151 [Didenko].

²⁴ IOSCO, *supra* note 22 at 21.

²⁵ Nakamoto, *supra* note 14 at 1.

²⁶ See Dirk A Zetzsche, Ross P Buckley and Douglas W Arner, "The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain" (2018) *U Ill L Rev* 1361 at 1372.

²⁷ See European Parliament, "Remaining Regulatory Challenges in Digital Finance" (Study, 30 April 2023) at 28–29 [Regulatory Challenges].

²⁸ See Hilary J Allen, "DeFi: Shadow Banking 2.0?" (2023) 64 *4 Wm & Mary L Rev* 919; Matteo Aquilina *et al*, "Decentralized Finance (DeFi): A Functional Approach" (2024) 10 *1 Journal of Financial Regulation* 1.

²⁹ These include, for instance, the manipulation of "oracles" responsible for fetching real-world data and providing them to the DeFi smart contracts. Malicious actors may also take control over a sufficient share of the protocol's governance tokens, thereby manipulating governance decisions for their own benefit. See Maya Dotan, Aviv Yaish, Hsin-Chu Yin, Eytan Tsytkin and Aviv Zohar, "The Vulnerable

the seller, attacks can focus on them.³⁰ With peer-to-peer decentralisation, there is a higher number of such weak pairs compared to traditional finance, which relies on robust, centralised counterparties. Human error or dishonesty also affects DeFi as it does any other system. Erroneous or malicious code can be introduced into smart contracts³¹ or other decentralised applications during the development process, leading to so-called “smart contract exploits”.³²

The emerging picture is of a brightly innovative and promising industry with significant challenges to overcome in a high-risk environment, combined with low trust in conventional risk-mitigating approaches. Within a few years, similar attacks have targeted several DeFi platforms, casting doubt on the industry’s ability to learn.³³ This may explain why the years 2022–2024, despite contracted asset prices during the crypto winter, were the worst years on record for crypto crime. During this period, illicit recipients accumulated approximately US\$150bn worth of crypto-assets.³⁴ Exposures like these carry the risk of knock-on effects across interconnected DeFi systems. These effects may even spread into the conventional financial system,³⁵ as some argue occurred in the run-up to the collapse of Silicon Valley Bank.³⁶

Thus, legislators are faced with a dilemma between strictly regulating the immature DeFi industry to address immediate risks and facilitating its out-of-the-box innovation. In this context, the US’s newfound crypto libertarianism may simply accept some short-term risks for eventual crypto hegemony, thus losing the battle yet winning the war – unless, to quote a famous European, “in the long run we are all dead.”³⁷

Nature of Decentralized Governance in DeFi” in *DeFi ‘23: Proceedings of the 2023 Workshop on Decentralized Finance and Security* (New York: Association for Computing Machinery, 2023) at p 25–31, available in ACM Digital Library, <https://dl.acm.org/doi/10.1145/3605768.3623539>.

³⁰ Regulatory Challenges, *supra* note 27. One example is “hot wallet attacks”, whereby hackers steal private keys from wallets while they are online; *Ibid* at 34.

³¹ Schär, *supra* note 13; Primavera De Filippi *et al*, “Smart Contracts” (2021) 10 2 Internet Policy Review, available in Internet Policy Review, <https://doi.org/10.14763/2021.2.1549>.

³² Sarwar Sayeed, Hector Marco-Gisbert and Tom Caira, “Smart Contract: Attacks and Protections” (2020) 8 IEEE Access, available in IEEE Xplore, <https://doi.org/10.1109/ACCESS.2020.2970495>.

³³ Regulatory Challenges, *supra* note 27 at 34 (also providing an overview of major asset misappropriations in DeFi). Similar failings of DeFi are also seen outside of the cybersecurity domain. See *eg*, Dirk A Zetsche, Ross P. Buckley, Douglas W Arner and Linus Föhr, “The ICO Gold Rush: It’s a Scam, It’s a Bubble, It’s a Super Challenge for Regulators” (2019) 63 2 Harv Intl LJ 267.

³⁴ Chainalysis, “2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized”, <<https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/>>. For examples and implications, see Regulatory Challenges, *supra* note 27 at 33–41.

³⁵ DORA at (3); Ross P Buckley, Douglas W Arner, Dirk A Zetsche and Eriks Selga, “Techrisk” (2020) Sing JLS 35 [Buckley, Arner and Zetsche, “Techrisk”]; Zetsche, Arner and Buckley, *supra* note 13 at 172–203.

³⁶ New York Times, “Silicon Valley Bank Collapse Sets Off Blame Game in Tech Industry” <<https://www.nytimes.com/...html>> (11 March 2023).

³⁷ John Maynard Keynes, *A Tract on Monetary Reform* (UK: Macmillan, 1923), ch 3.

B. The Digital Operational Resilience Act on DeFi

The cyber resilience approach of DORA extends to a broad range of financial entities, making compliance with DORA a prerequisite for offering financial services to 500 million affluent European consumers and the institutional investors managing their pensions. This incentivises global businesses to build DORA-compliant resilience into their technology and processes. Financial institutions rely on complex and interconnected technology around the world, often delivered by global third-party technology and cloud service providers.³⁸

DORA is inspired by “relevant international, national and industry best practices, guidelines, recommendations and approaches”,³⁹ including the latest work of the Bank for International Settlements (“BIS”) and IOSCO.⁴⁰ DORA-compliant services are also likely to extend far beyond Europe, a phenomenon referred to by Anu Bradford as the “Brussels Effect”, which assigns the EU a *de facto* role as a global regulator in certain areas, where firms have an incentive to apply equivalent rules outside Europe.⁴¹ This influence may accelerate as DORA’s principles shape recommendations by IOSCO, BIS and similar regulatory bodies that many regulators, including in the US, look to for guidance.

Aiming at the entire financial industry, DORA demands compliance in the field of DeFi as well. Here, one could argue that the need for internationally harmonised regulation is particularly acute, while the innovative strength of regulatory competition may be required to keep pace with technological progress. The next section explores the tensions between DORA’s risk management approach, which positions financial institutions at the top of a risk management hierarchy, and the peer-to-peer, cooperative and decentralised nature of crypto.

³⁸ Financial Stability Institute, *supra* note 21; Scott, *supra* note 15; Kun, *supra* note 15; European Securities and Markets Authority, *Joint ESA Response to the European Commission’s February 2021 Call for Advice on Digital Finance and Related Issues: Regulation and Supervision of More Fragmented or Non-integrated Value Chains, Platforms and Bundling of Various Financial Services, and Risks of Groups Combining Different Activities* (Joint Report, ESA 2022 01, 31 January 2022); European Securities and Markets Authority, *Joint ESA Report on 2023 Stocktaking of BigTech Direct Financial Services Provision in the EU* (Joint Report, JC 2024 02, 2024).

³⁹ DORA, *supra* note 2 at (47); See also DORA, *supra* note 2 at Art 18(4), Art 33(3)(i), Art 44, (56), (94).

⁴⁰ For instance, DORA visibly draws from the recommendations outlined in Financial Stability Institute, *supra* note 21 and Committee on Payments and Market Infrastructures, “Guidance on Cyber Resilience for Financial Market Infrastructures” <<https://www.bis.org/cpmi/publ/d146.htm>> (29 June 2016).

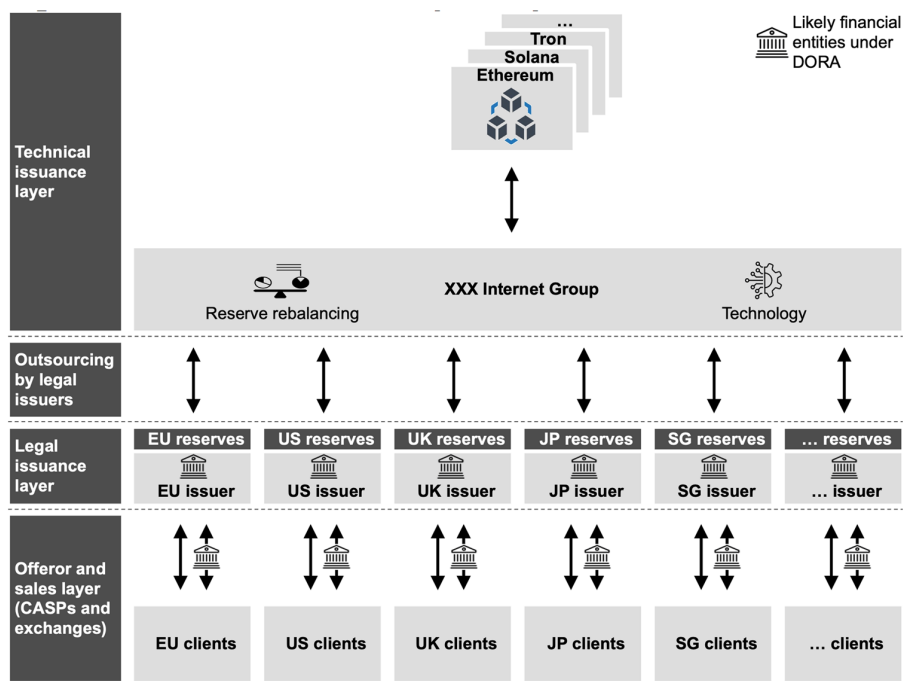
⁴¹ Anu Bradford, “The Brussels Effect” (2012) 107 1 Nw UL Rev 1. The Brussels Effect is derived from five elements: the EU’s large market size, its regulatory capacity, its tendency to apply more stringent standards than other jurisdictions, the difficulty (or inelasticity) of businesses to avoid regulation, and the incentive for businesses to standardise and thus apply the same standards globally. See also Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford: Oxford University Press, 2020) ch 2, 5; Annegret Bendiek and Isabella Steuerzer, “The Brussels Effect, European Regulatory Power and Political Capital: Evidence for Mutually Reinforcing Internal and External Dimensions of the Brussels Effect from the European Digital Policy Debate” (2023) 2 5 Digital Society 4.

C. CeFi and DeFi as Two Sides of the Same Coin

Influential commentators⁴² and regulatory approaches⁴³ distinguish between more centralised crypto setups characterised by a single issuer, which we refer to as CeFi, and more decentralised approaches referred to as DeFi in the strict sense. This distinction is important for the regulation of the issuers themselves and their products, since someone must implement and be held accountable for complying with product-related regulations. However, we argue that for cyber resilience the difference between CeFi and DeFi is of secondary importance. This is because the service chain in both CeFi and DeFi setups ultimately relies on the cooperation of peers in non-hierarchical networks. We take this position against the backdrop of stablecoin setups, which are among the most centralised crypto arrangements, and of crypto lending, where a decentralised setup has become widely accepted.

In a centralised crypto scheme, we may find a setup like that in Figure 1, drawing on stablecoins like Circle.

Figure 1: Global Stablecoin Set-up Example



Source: Dirk A. Zetzsche, “Third-country Multi-issuer Stablecoins” (2025) 27 ERA Forum 165 at 169, available in Springer Nature Link, <https://doi.org/10.1007/s12027-025-00866-4>.

⁴² See eg, Katrin Schuler, Ann Sofie Cloots and Fabian Schär, “On DeFi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance” (2024) 10 2 Journal of Financial Regulation 213.

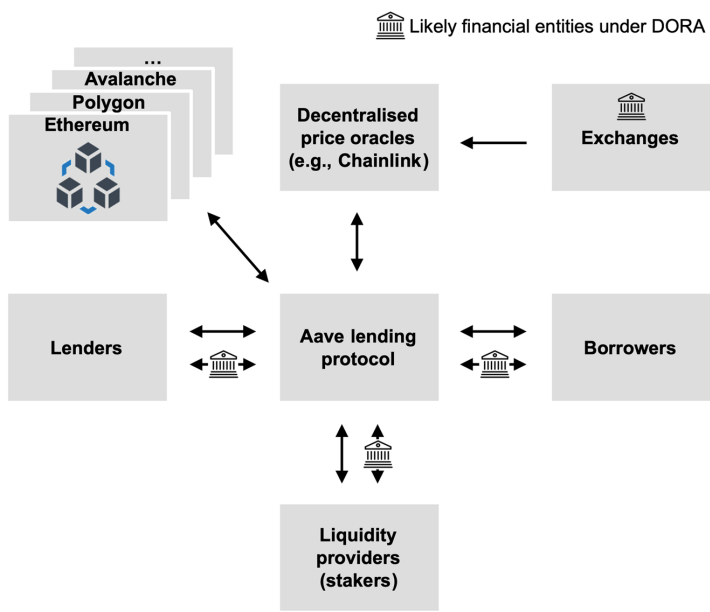
⁴³ See eg, MiCA, at (22).

In a stablecoin setup, the crypto-asset service providers (“CASPs”) trade and often hold crypto on behalf of their clients. The crypto-assets delivered to the CASPs are generated and provided by processes legally controlled by the issuer, which is usually a financial institution subject to DORA.⁴⁴ However, the issuers typically do not perform the technical processes of issuance and redemption themselves. Instead, a technology firm operates behind the issuer, managing a network of various entities that collectively create (mint) and issue or redeem and destroy (burn) the respective stablecoin. This firm also connects to multiple DeFi platforms where the stablecoins are used as a cash substitute.

Importantly, neither the technology firm nor the network partners upstream, who connect to the DeFi platforms that utilise the stablecoins, are directly subject to DORA’s risk management requirements. This lack of oversight exists either because these partners are in non-EU jurisdictions or because they provide purely technical rather than financial services. Nevertheless, without the cooperation of all these regulated and unregulated entities stablecoins would not be accepted by millions of users globally.⁴⁵

In contrast, a fully decentralised crypto scheme may resemble the setup illustrated in Figure 2, using the crypto lending platform Aave as an example.

Figure 2: Aave Lending Platform Example



In a DeFi lending setup, liquidity providers, which may or may not be financial institutions and as such subject to DORA, and CASPs interact with a decentralised

⁴⁴ DORA, at Art 2(1)(a), (d), (f) *cf* MiCA, 9 at Art 48.
⁴⁵ For details, Dirk A Zetzsche, “Third-country Multi-issuer Stablecoins” (2025) 27 ERA Forum 165, available in Springer Nature Link, <https://doi.org/10.1007/s12027-025-00866-4>.

network of servers. This network runs code that coordinates lending and borrowing among various clients without the need for its own balance sheet. One can draw parallels to crowd lending, yet entirely operated by code, where both lenders and liquidity providers are crowdsourced. In this system, lenders can deposit crypto-assets into a pool and withdraw them at will with interest, while others can borrow from the pool and repay with interest.⁴⁶ They may use CASPs to facilitate transactions, but it is also possible to transact directly on-chain with the decentralised pool. Notably, the only entities subject to DORA are peripheral to the core lending activity, if they are present at all, while the DeFi lending platform itself is possibly not regulated as a financial institution and thus not subject to DORA. This conclusion arises either because a fully decentralised network of multiple entities lacks a single entity that could be regulated if we disregard the code developers, or because the activity itself is not regulated.⁴⁷

Ultimately, this situation mirrors that of stablecoins. At some point in the service chain, the hierarchical structure of financial institutions and clients concludes, and an intense collaboration among various technology services and providers takes its place. This context sets the stage for our inquiry into the effectiveness of DORA-style risk management requirements in DeFi.

III. THE DIGITAL OPERATIONAL RESILIENCE ACT AND ITS IMPACT ON DeFi

In this section, we introduce the scope of DORA before analysing its impact on DeFi and the “DeFi Stack.”

A. *The “Five Pillars” of the Digital Operational Resilience Act*

DORA’s tools are commonly referred to as its “five pillars”, which are outlined in Chapters II to VI of the regulation (see Figure 3).

Firstly, DORA mandates that the “management body” of the financial institution engages in ICT risk management, primarily through strategy and governance requirements,⁴⁸ as is the case with other cybersecurity laws.⁴⁹ Secondly, the financial institution must ensure effective cyber incident management, classification, and reporting to the board and supervisory authorities throughout the EU. Thirdly, DORA introduces mandatory resilience testing, which includes advanced threat-led penetration testing (“TLPT”), a rigorous cybersecurity exercise that simulates real-world advanced cyberattacks. Fourthly, DORA places significant emphasis on ICT

⁴⁶ Global X Research Team, “Aave: The Basics” <<https://www.globalxetf.com/articles/aave-the-basics>> *Global X* (14 March 2023).

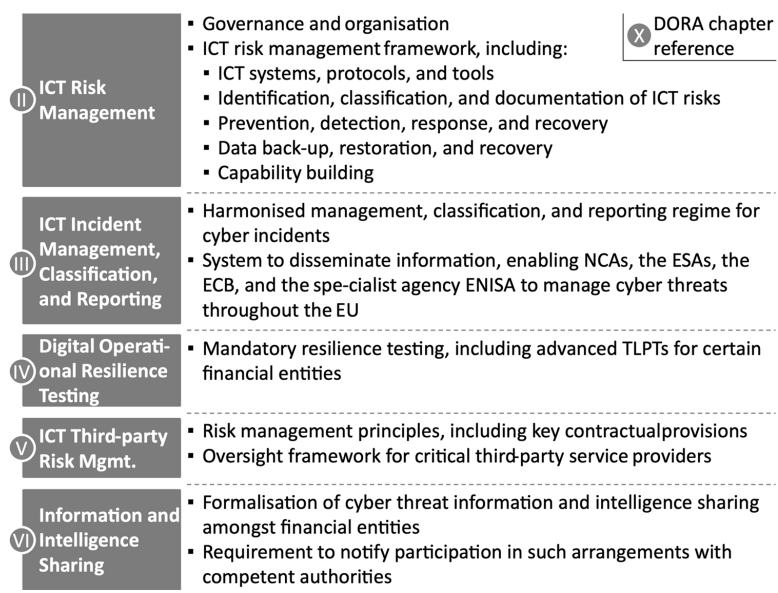
⁴⁷ Note that we do not take a stance here on whether Aave is, in fact, fully decentralised or whether their activity is regulated or not, for instance as provision of credit. See on these questions, Zetzsche and Woxholth, *supra* note 3 at 45–46, 103–104.

⁴⁸ DORA, at Art 5, (45)–(47).

⁴⁹ Financial Stability Institute, *supra* note 21 at 15–16; Didenko, *supra* note 23 at 139–140.

third-party risk, which not only encompasses standard risk management but also establishes a new oversight framework for critical ICT third-party service providers. DORA was specifically designed with cloud service providers such as Amazon, Microsoft and Google in mind.⁵⁰ Chapter VI DORA formalises information sharing among financial institutions regarding cyber threats to address confidentiality and anti-trust concerns, facilitating essential collaboration on cybersecurity.⁵¹

Figure 3: The “Five Pillars” of DORA



Source: Inspired by Zetzsche and Woxholth, *supra* note 3 at 249.

DORA’s five pillars assume that financial institutions possess the means and information necessary for compliance and can effectively direct and instruct their service providers. However, this assumption is questionable in the context of DeFi, where cooperation often replaces traditional hierarchy. In particular, DeFi relies heavily on third-party services offered by various entities each of which operates on a scale very different from that of global cloud service providers, and TLPT also has limited utility if only part of the DeFi network participates, especially considering that the public blockchains may consist of tens of thousands of servers globally. The use of open-source code and informal networks prevalent in DeFi also conflicts with the need to share confidential information about cyber threats, which may come with price-sensitive information.

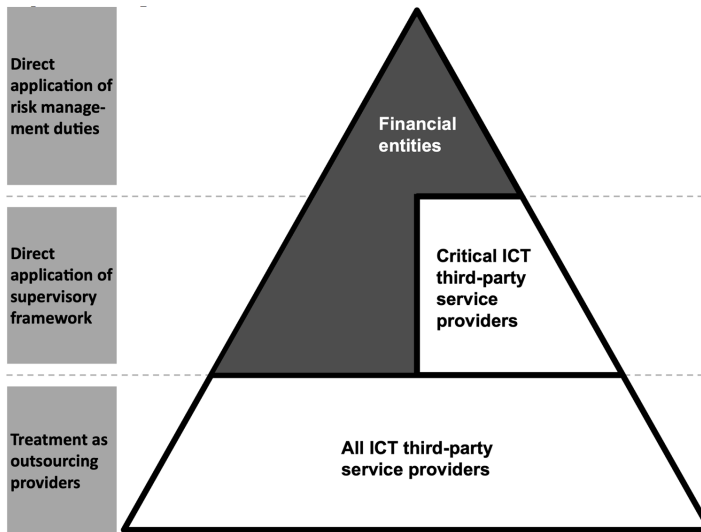
⁵⁰ DORA, at (20).

⁵¹ *Ibid* at Art 45.

B. The Digital Operational Resilience Act's Scope

The potential mismatch between regulatory expectations and reality may be addressed by DORA's scope. DORA applies to licensed financial entities and "critical" ICT third-party service providers (see Figure 4).

Figure 4: Scope of DORA



Article 2(1)(a) to (t) of DORA lists 23 types of “financial entities” recognised under EU law,⁵² with updates expected once the Financial Data Access Regulation (“FIDA”) is adopted. The scope includes all MiCA-licensed issuers and CASPs. DORA is part of financial supervision, with the competent authorities designated for MiCA entities responsible for enforcement.⁵³

DORA lightens requirements for microenterprises with fewer than ten employees and an annual turnover and/or balance sheet below €2m, unless they operate a trading venue or central counterparty.⁵⁴ In line with common practice elsewhere,⁵⁵ DORA also imposes a broad proportionality principle.⁵⁶ The following section examines both of these aspects in greater detail.

⁵² *Ibid* at Art 2(2), *cf Ibid* at Art 2(1) (a)-(t), Art 3. This list will be expanded to 24 types with the new Financial Data Access Regulation (“FIDA”). See European Commission, Proposal for a Regulation on a Framework for Financial Data Access, [2020] at (32), Art 35, <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020PC0595>> (accessed 18 July 2026).

⁵³ DORA, *supra* note 2 at Art 46(d).

⁵⁴ *Ibid* at Art 3(60); the further exemptions for trade repositories and central securities depositaries have no practical meaning.

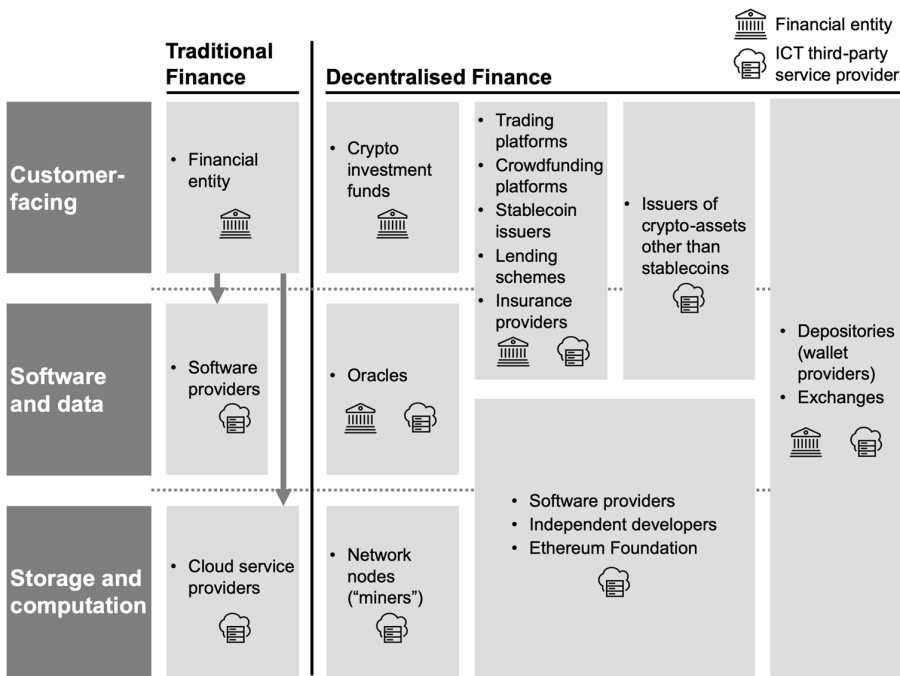
⁵⁵ See Financial Stability Institute, *supra* note 21 at 27.

⁵⁶ See DORA, *supra* note 2 at Art 4, which applies to Chapters II to IV and Section I of Title V DORA. For ICT third-party service providers, an even stronger proportionality principle applies by the very fact that DORA extends only to those service providers that are designated as “significant” according to its Art 31.

Financial entities at the top of the hierarchy are expected to manage ICT risks related to both their internal and third-party ICT services.⁵⁷ Some of these providers may qualify as delegates under EU financial law and, as such, be subject to instructions from the financial entity.⁵⁸ However, many ICT services will not qualify, which is why DORA adopts a tailored approach to integrate these services into the financial entity’s overall risk management framework under the five pillars of DORA outlined above.

DORA’s definition of ICT services is broad.⁵⁹ It includes, for instance, cloud computing, software, data analytics and data centre services.⁶⁰ Once a participant in a network qualifies as a financial entity, many other parts of the network may qualify as its ICT third-party service providers under DORA (see Figure 5).

Figure 5: Typical Relationships in Traditional Finance versus DeFi



In addition, DORA imposes direct oversight on “critical” ICT third-party service providers.⁶¹ The designation of an ICT service provider as critical largely depends

⁵⁷ See *Ibid* at Art 3(19), 3(20), 6(10), 19(5), and 28(1)(a). Intra-group service providers cannot be designated as “critical”, see DORA, at Art 31(8)(iii).

⁵⁸ The discussion of whether the reliance on mere data and software services qualify as delegations under EU law is ongoing. *Cf.* in the context of risk management, Dirk A Zetzsche and M Hanke, “Risk Management” in *The Alternative Investment Fund Managers Directive* (Dirk A Zetzsche, ed(s)) (Alphen aan den Rijn: Wolters Kluwer, 3d ed, 2020) ch 13 at 329 *et seq.*

⁵⁹ DORA, at (35).

⁶⁰ *Ibid* at (63).

⁶¹ *Ibid* at Art 31–44.

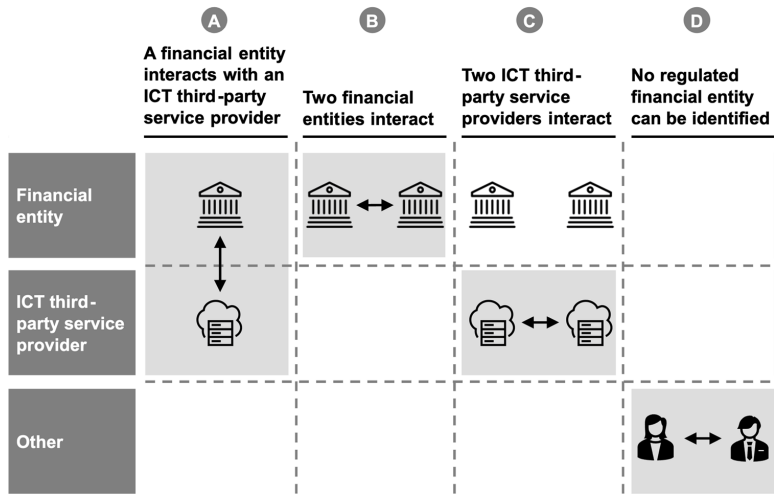
on the systemic impact of the provider and the reliance of financial entities on its services.⁶² DORA’s geographical scope encompasses all ICT third-party service providers to in-scope “financial entities”, regardless of the provider’s own jurisdiction. This global reach is intentional, as many large service providers, especially in the cloud sector,⁶³ reside outside the EU.⁶⁴

The list of “critical” providers published by the Joint Committee of the European Supervisory Authorities includes 19 prominent firms in telecommunications, cloud, operating systems, and financial data.⁶⁵ These services are vital for DeFi (for instance, much of DeFi relies on telecom and cloud services); however, no specific DeFi entity is classified as a critical ICT service provider.

Considering these factors collectively, we identify four scenarios under DORA:

- (a) A financial entity interacts with an ICT third-party service provider.
- (b) A financial entity interacts with another financial entity.
- (c) Two ICT third-party service providers interact.
- (d) No regulated financial entity can be identified (see Figure 6).⁶⁶

Figure 6: Relationships under DORA



Source: Zetzsche and Woxholth, *supra* note 3 at ch 14.

⁶² *Ibid* at Art 31(2); European Commission, Commission Delegated Regulation (EU) 2024/1502 of 22 February 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council by specifying the criteria for the designation of ICT third-party service providers as critical for financial entities, [2024] OJ L 2024/1502, 30 May 2024.

⁶³ DORA, at (20). One can speculate that DORA here also aims to support European financial entities in negotiating better terms on cybersecurity with American “Big Tech” as alluded to in Recitals 28 and 30 DORA.

⁶⁴ Technically, this is achieved by means of Art 31(12) DORA, which mandates financial entities to use only those critical ICT third-party service providers who establish a subsidiary in the Union.

⁶⁵ European Insurance and Occupational Pensions Authority, “List of designated CTPPs” <<https://www.eba.europa.eu/sites/default/files/2025-11/e388451b-356b-408a-bbf2-b8e425865d75/List%20of%20designated%20CTPPs.pdf>> (18 November 2025).

⁶⁶ Zetzsche and Woxholth, *supra* note 3 at 260.

In scenarios (a) and (b), each financial entity is accountable for its own compliance, as well as that of its ICT third-party service providers, but not for the service providers of other financial entities. In scenario (c), neither party has risk management obligations under DORA, as these are solely the responsibility of financial entities. In scenario (d), the network falls outside DORA's scope. Therefore, DORA's impact on DeFi hinges on the identification of a "financial entity", an "ICT third-party service provider" or the lack thereof, which we will discuss in the next section.

C. Crypto Activities and Services Under the Digital Operational Resilience Act

Financial entities that serve as the entry point for DORA duties include issuers of asset-referenced tokens ("ARTs") and e-money tokens ("EMTs"), CASPs and other licensed financial entities.

1. Crypto asset issuers

All issuers of so-called stablecoins under MiCA fall within the scope of DORA. This includes issuers of ARTs (which may or may not be credit institutions) as well as credit institutions and e-money institutions entitled to issue EMTs under MiCA.⁶⁷ EMTs replicate and represent a single currency, such as the USD, whereas ARTs represent other assets, such as gold or a basket of several assets, as exemplified by the infamous Libra project.⁶⁸

DORA also applies to some ARTs that are issued in a decentralised manner, as the authorisation requirement under Article 16(1) MiCA extends to "other undertakings" in addition to legal persons. This is interpreted as referring to a relatively stable group of developers and/or operators who jointly control the DeFi application.⁶⁹

DORA does not apply to the issuance of "other" crypto-assets, which are addressed under Title II MiCA. The same applies to issuers of crypto-assets exempt from MiCA, such as non-financial tokens subject to Article 2(3) MiCA or fully decentralised crypto-assets that lack an issuer and any control-holder, such as Bitcoin and Ether.⁷⁰

Stablecoins act as currency within DeFi systems; they are used, for example, to pay for (other) crypto-assets or crypto-asset services, not only in centralised crypto-asset services but also in fully decentralised DeFi lending schemes and

⁶⁷ DORA, at Art 2(1)(a), (d), (f), *cf* MiCA, *supra* note 9 at Art 48.

⁶⁸ MiCA, Art 3(1)(6), (7); Dirk A Zetsche, Ross P Buckley, and Douglas W Arner, "Regulating Libra" (2021) 41 1 Oxford J Leg Stud 80.

⁶⁹ Zetsche and Woxholth, *supra* note 3 at 79–81. The US GENIUS Act is more liberal as it exempts developers of stablecoins explicitly from functioning as issuer.

⁷⁰ MiCA, at (22), (26).

applications.⁷¹ As a result, depending on the context, other parts of the DeFi network may qualify as the ART or EMT issuers' "ICT third-party service providers". We will discuss this relationship in more detail in Part III.D below.

2. *Crypto-asset service providers*

CASPs authorised under Title V MiCA qualify as "financial entities" under DORA.⁷² They are defined as providers of one or more specified services, including custody, operating a crypto-exchange, exchanging crypto for crypto and non-crypto funds, executing crypto orders, and placing, receiving, or transmitting orders related to crypto-assets, as well as providing crypto advice, portfolio management, or transfer services for clients.⁷³ Notably, crypto lending and staking as well as bridging and mixing services are not categorised as crypto-asset services. For example, the core lending activity in the above Aave example is not regulated. However, entities and organised groups offering these services fall within the scope if they involve, for instance, the transfer of crypto-assets, the exchange of crypto for crypto or the reception, transmission or execution of orders related to crypto.⁷⁴

It is important to note that providing regulated services in a decentralised manner does not inherently exempt one from being classified as a financial entity. Developers or operators of a protocol (*ie*, software) who jointly control aspects of a DeFi network, whether through technical means, factual control, the use of "golden tokens", access to the source code or voting majorities,⁷⁵ may be classified as a CASP under MiCA and consequently as a "financial entity" under DORA.⁷⁶

3. *Other financial entities in DeFi*

MiCA's scope does not extend to financial institutions licensed under EU financial law.⁷⁷ When DeFi protocols replicate the services of conventional financial entities, such as investment services related to financial instruments, these DeFi services must adhere to the applicable EU financial law for such services, with their providers being subject to DORA as financial entities. The provision of insurance services,

⁷¹ Gary B Gorton and Jeffery Y Zhang, "Taming Wildcat Stablecoins" (2023) 90 3 U Chicago L Rev 909; Douglas W Arner, Raphael Auer, and Jon Frost, "Stablecoins: Risk, Potential, and Regulation" University of Hong Kong Faculty of Law Legal Studies Research Paper Series (2020), available in SSRN eLibrary, <https://dx.doi.org/10.2139/ssrn.3979495>.

⁷² DORA, at Art 2(1)(f).

⁷³ MiCA, at Art 3 (15), (16).

⁷⁴ For a detailed discussion see Zetzsche and Woxholth, *supra* note 3 at 95–105.

⁷⁵ Linn Anker-Sørensen and Dirk A Zetzsche, "From Centralized to Decentralized Finance: The Issue of 'Fake-DeFi'" (2021) SSRN Electronic Journal, available in SSRN eLibrary, <http://dx.doi.org/10.2139/ssrn.3978815>; Mitchell Goldberg and Fabian Schär, "Metaverse Governance: An empirical analysis of voting within Decentralized Autonomous Organizations" (2023) 160 Journal of Business Research 113764, available in ScienceDirect, www.sciencedirect.com/science/article/pii/S0148296323001224.

⁷⁶ Art 59 (1)(a) MiCA includes "other undertakings". See Zetzsche and Woxholth, *supra* note 3 at 95–105, 261–262.

⁷⁷ See MiCA, at Art 2(4).

moreover, is exempt from MiCA,⁷⁸ but entities that offer or facilitate guarantees or assume risk in DeFi schemes may qualify as insurance or reinsurance undertakings under EU law and, as such, still be subject to DORA.⁷⁹ This could place certain issuers of crypto derivatives within its scope. Similarly, an entity operating scoring and rating engines for evaluating creditworthiness in DeFi may potentially be classified under DORA as a “credit rating agency”.⁸⁰ While crypto-asset lending and borrowing are exempt from MiCA,⁸¹ such activities could result in “financial entity” status as a credit institution⁸² if the underlying debt is offered or written in fiat currency before the transaction is executed in crypto-assets.

It is important to note that the application of the CASP definition requires careful consideration. For example, portfolio management under the CASP definition refers specifically to “mandates given by clients on a discretionary client-by-client basis.”⁸³ Nevertheless, managers of crypto-asset investment funds that qualify as alternative investment fund managers (“AIFMs”) are subject to DORA due to their regulatory status as AIFMs.⁸⁴ Similarly, crowdfunding services lacking a placing commitment that fall outside the CASP definition’s reference to “placing of crypto-assets” are also subject to DORA, as Article 2(1)(s) DORA includes crowdfunding service providers under the European Crowdfunding Service Provider Regulation.⁸⁵

Even if an activity requires licensing under EU financial law, DORA exempts certain financial entities, which are generally small.⁸⁶ This results in full exemptions from DORA for, *eg*, small managers of alternative investment funds, small insurance intermediaries and small investment firms. EU Member States may also exempt small institutions that engage in credit provision functions. These exemptions are a crucial aspect of ensuring the proportionality of DORA, as discussed in the next section.

⁷⁸ Cf MiCA, at Art 2.

⁷⁹ DORA, at Art 2(1) (n), (o), cf *Ibid* at Art 2(2)(b) and 2(2)(e) and Art 3(47)–(51), with further references to Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance, OJ 2009 No L335 (Solvency II) and Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution, OJ 2016 No L26.

⁸⁰ See DORA, Art 2(1)(q), cf *Ibid* at Art 3(54).

⁸¹ MiCA, at (94).

⁸² DORA, at Art 2(1)(a).

⁸³ MiCA, Art 3(1)(16)(i), cf *Ibid* at Art 3(1)(25).

⁸⁴ See DORA, at Art 2(1)(k), 3(44), cf Alternative Investment Fund Managers and amending Directives, EU Parliament and Council Directive 2011/61/EU at p16, [2011] OJ L 174/1 at Art 4(1)(b), <<https://eur-lex.europa.eu/eli/dir/2011/61/oj/eng>> (accessed 18 July 2026). On details, see D.A. Zetzsche, Filippo Annunziata, Julia Sinnig, “Digital Assets, MiCA & EU Investment Fund Law” (2025) 26(3) EBOR 497.

⁸⁵ European Crowdfunding Service Providers Regulation, EU Parliament and Council Regulation 2020/1503, [2020] OJ L 347/1, <<https://eur-lex.europa.eu/eli/reg/2020/1503/oj/eng>> (accessed 18 July 2026).

⁸⁶ Cf DORA, *supra* note 2 at Art 2(3) and (4).

4. *Proportionality and openness to innovation*

The interconnectedness among financial entities and their service providers means that even a threat to smaller entities could affect the entire system. Thus, apart from the bespoke exemptions for very small intermediaries discussed in the previous section, DORA does not offer general exemptions for small entities, but it does provide partial exemptions for microenterprises⁸⁷ alongside a general principle of proportionality.⁸⁸ This aligns with the regulatory approach to cybersecurity adopted elsewhere.⁸⁹

However, applying proportionality is challenging due to the high level of interconnectedness among network partners⁹⁰ as well as the presence of systemically important crypto intermediaries (“SICIs”) at the heart of crypto ecosystems.⁹¹ Should supervisors focus on the network characteristics, where many small actors must participate to achieve positive decentralisation effects, or on the size and capacities of individual actors?⁹²

Notably, DORA does not provide size-based exemptions for DeFi. In the DeFi space, many individuals or small developer firms actively participate in the development or operation of applications. Given the various entry points for DORA’s scope (as an ART issuer, CASP, or in relation to traditional licensed activities), the partial exemption for microenterprises is significant. Entities with fewer than ten employees may be relieved from certain compliance burdens as microenterprises. For example, they are exempt from the requirement to establish a role and independent function to monitor relationships with third-party ICT service providers.⁹³ The revision of the ICT risk management framework does not need to occur annually nor require a regular audit by an independent auditor.⁹⁴ When there is a major change, and during the annual risk assessment of all legacy ICT systems, the requirements are lighter.⁹⁵ Nonetheless, these and other⁹⁶ deviations do not alter the reality that even the smallest entities in the scope of MiCA, including those with just one developer, are subject to DORA, while most other very small financial entities under EU financial law are exempt.⁹⁷

⁸⁷ Microenterprises are defined in DORA, at Art 3(60).

⁸⁸ DORA, at Art 4.

⁸⁹ Financial Stability Institute, *supra* note 21 at 27.

⁹⁰ The simplified ICT risk management framework in Art 16 DORA applies, for instance, to “small and non-interconnected investment firms”, thus requiring investment firms that are interconnected with a larger DeFi network to apply the more comprehensive ICT risk management framework in Articles 5 to 15 DORA.

⁹¹ Douglas W Arner, Dirk A Zetsche, Ross P Buckley, and Jamieson M Kirkwood, “The Financialization of Crypto: Designing an International Regulatory Consensus” (2024) 53 Computer L & Sec Report 105970, available in ScienceDirect, <https://doi.org/10.1016/j.clsr.2024.105970>.

⁹² In supervisory releases, we have not identified any example relevant to DeFi where proportionality justified the non-application of DORA.

⁹³ DORA, at Art 5(3) and 6(4).

⁹⁴ *Ibid* at Art 6(4)–6(6).

⁹⁵ *Ibid* at Art 8(3), 8(7), 11(3).

⁹⁶ *Ibid* at Art 11(7), 11(10), 12(4), 13(2), 13(7), 24(1), 24(3)–24(6), 26(1), 28(2), 30(3).

⁹⁷ *Cf Ibid* at Art 2(3) and 2(4). This different treatment of small MiCA-licensed firms is likely to be copied into FIDA. See European Commission, at Art 2(3), *cf* Art 2(2) (e) and (f).

Although DORA acknowledges that outsourcing enables small financial entities to deliver resilient digital financial services, it still requires these entities to exercise caution when selecting qualified and compliant service providers.

While both proportionality and written exemptions offer limited relief, DORA allows for a purpose-oriented interpretation of the binding texts. Reflecting rapid technological and business model innovations, DORA's risk management obligations for financial entities focus on strategy and governance rather than on specific technical requirements. Even when regulating ICT systems, protocols and tools, DORA mandates that these be "appropriate", "reliable", or "sufficient" or applies similar and deliberately vague standards whose meanings may evolve over time.⁹⁸

Indeed, the widespread use of general and intentionally vague standards is a built-in feature of DORA's risk management framework, which must itself be "sound, comprehensive and well-documented".⁹⁹ Similar standards apply to each of its components outlined in Articles 7 to 14 of DORA. This vague, procedural approach is necessary in legal requirements within a rapidly changing field such as cybersecurity, especially when coupled with another innovative sector like DeFi. Nevertheless, apart from specific exemptions for microenterprises, DORA applies fully to both large and small financial entities within DeFi networks.

5. Fully decentralised services

MiCA's exemption for fully decentralised services has a parallel in DORA's focus on the "financial entity" as the subject of regulation.¹⁰⁰ By assigning risk management obligations solely to "financial entities", so-called "fully decentralised services" are presumably exempt from DORA, as no identifiable financial entity exists in these cases. Consequently, no part of the network can be classified as an ICT third-party service provider, since these providers, by definition, offer services to financial entities.

We anticipate that many participants in DeFi networks will seek refuge under MiCA's exemption for fully decentralised services, and we expect similar behaviour concerning DORA.¹⁰¹ For DORA to be effective, it will be essential to draw a clear distinction, ensuring that only genuinely decentralised services qualify for the MiCA exemption, as the implications extend beyond MiCA to DORA.

The same legal challenge, the absence of a delegate acting as a counterparty, may arise when financial entities depend on decentralised services further up the chain. Examples include CASPs holding assets for clients traded on decentralised exchanges, clients instructing the CASP to transfer crypto-assets via decentralised mixers and bridges, technology firms collaborating with a wide network of smaller decentralised ecosystems to ensure the use and fungibility of stablecoins (see Figure 1 above) or licensed investment firms, fund managers, and credit institutions

⁹⁸ DORA, at Art 7.

⁹⁹ *Ibid* at Art 6(1).

¹⁰⁰ See MiCA, at Art 2(1), by which it applies to "natural and legal persons and certain other undertakings", along with MiCA at (22), (26), Art 4(3)(b); Zetzsche and Woxholth, *supra* note 3 at 45–46.

¹⁰¹ Zetzsche and Woxholth, *supra* note 3.

acting as lenders on decentralised lending platforms (see Figure 2 above). Even when a licensed activity exists, and the next level up qualifies as an ICT service in relation to the former, the efficacy of DORA-style risk management remains questionable when decentralisation is present in the entity's operations. We will discuss these situations in the next section.

D. *ICT Third-Party Services in a DeFi Context*

We will examine in turn the presence of ICT third-party service providers in DeFi setups, considering the broad DORA definition of ICT services outlined above in Section III.B.

1. *ICT services*

ICT services are defined as:

Digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services.¹⁰²

This definition blurs the boundaries between financial entities and their service providers, hence the reference to both “internal and external” users.¹⁰³ The terms “financial entity” and “ICT third-party service provider” are also not mutually exclusive, meaning the same entity can be both a financial entity under DORA and an ICT third-party service provider for another financial entity.¹⁰⁴ This situation is common in DeFi, where many entities provide a combination of ICT services, by way of data exchange, coding or provision of server capacity, and financial services within these networks. For example, crypto exchanges typically qualify as CASPs under MiCA and, therefore, as financial entities under DORA. However, in our earlier example of Aave, they only offer price information through the technological interlinkages that support transactions on the Aave platform.

Any licensed financial service mentioned in Article 2(1) DORA that comes with an ICT component does not qualify as an ICT service under DORA,¹⁰⁵ yet for unrelated or independent services of the same financial entity, any ICT service, that

¹⁰² DORA, at Art 2(1)(u), *cf* DORA at Art 3(19) and 3(21).

¹⁰³ DORA distinguishes between third-party and intra-group ICT service providers. See *Ibid* at Art 3(19), 3(20). Intra-group service providers cannot be designated as “critical”, see *Ibid* at Art 31(8)(iii).

¹⁰⁴ See DORA, at (63); European Insurance and Occupational Pensions Authority, “DORA124-3169”, <https://www.eiopa.europa.eu/qa-regulation/questions-and-answers-database/dora124-3169_en> (16 October 2024); European Insurance and Occupational Pensions Authority, “DORA030-2999”, <https://www.eiopa.europa.eu/qa-regulation/questions-and-answers-database/dora030-2999_en> (14 February 2024) [DORA030-2999].

¹⁰⁵ DORA030-2999, *supra* note 104.

is any data exchange, provision of server capacity and computation power, coding or other contribution,¹⁰⁶ qualifies as ICT service under DORA.¹⁰⁷ Further, any third-party provider of independent “digital and data services” to a financial entity will be considered an “ICT third-party service provider” under DORA. This classification will apply to numerous entities within a DeFi network. Therefore, one EU bank participating in a DeFi network potentially prompts DORA duties relating to the whole network and must respond either by enhancing its own ICT risk management or applying ICT outsourcing rules, which may involve the providers of digital and data services. Adding “financial information service providers” to the list of Article 2(1) DORA, as is proposed by the European Commission,¹⁰⁸ would reduce the scope of outsourcing duties in theory; yet it does not mitigate the regulatory overreach in substance, as we hardly expect crypto community members to obtain a licence for financial information services, for lack of size and EU focus.

2. *Delivery on an ongoing basis*

DORA defines “ICT third-party service provider” as an “undertaking providing ICT services”.¹⁰⁹ Under EU financial law, the term “undertaking” implies a degree of continuity and a stable governance structure. DORA reinforces this by stipulating that ICT services must be delivered “on an ongoing basis”,¹¹⁰ so mere sporadic service delivery does not qualify. For example, the one-time provision of a DeFi dataset does not equate to service delivery, whereas connecting the DeFi network to the data stream of a crypto exchange using oracles would qualify as an ICT service.¹¹¹

In the DeFi space, some participants offer permanent services while others provide only sporadic ones, with the nodes of Bitcoin and Ether being notable examples.¹¹² Here, for an analogy, we refer to conventional cloud service providers, which offer ICT services under DORA continuously, even when the data stored are not actively used by the client, such as in a backup storage solution. Similarly, in DeFi, nodes store a copy of the blockchain and maintain its integrity on an ongoing basis, even if each node only occasionally updates the chain by adding a new block.¹¹³

¹⁰⁶ See Technical Standards for the application of Regulation (EU) 2022/2554, EU Commission Regulation 2024/2956, [2024] at Annex 3, <https://eur-lex.europa.eu/eli/reg_impl/2024/2956/oj/eng> (accessed 18 July 2026).

¹⁰⁷ DORA030 – 2999, *supra* note 104.

¹⁰⁸ FIDA.

¹⁰⁹ DORA, at Art 3(19).

¹¹⁰ *Ibid* at (35).

¹¹¹ See on oracles in DeFi, Abdelijalil Beniche, “A Study of Blockchain Oracles” (2020) arXiv <<https://doi.org/10.48550/arXiv.2004.07140>> (14 July 2020); Kamran Mammadzada, Mubashar Iqbal, Fredrik Milani, and Luciano García-Bañuelos, “Blockchain Oracles: A Framework for Blockchain-Based Applications” in *Business Process Management: Blockchain and Robotic Process Automation Forum* (Aleksandre Asatiani, José María García, Nina Helander, Andrés Jiménez-Ramírez, Agnes Koschmider, Jan Mendling, Giovanni Meroni, Hajo A Reijers, eds) (Princeton: Springer, 2020).

¹¹² Zetzsche and Woxholth, *supra* note 3 at 18–20.

¹¹³ *Ibid* at 262.

3. Liability for ICT third-party services

Financial entities cannot absolve themselves of liability under DORA by outsourcing ICT services, as they remain responsible for the compliance of both their internal and outsourced ICT operations.¹¹⁴ While DORA aligns with MiCA and other EU regulations in this regard, its focus on technology rather than financial services carries significant implications. Financial entities are accountable for the compliance of outsourced financial services under MiCA and other EU financial laws, and similarly they bear responsibility for outsourced ICT services under DORA. This represents a marked shift from previous practices where financial entities could safely rely on third parties to be responsible for ICT infrastructure such as telecommunications and computing systems.¹¹⁵

This is partially acknowledged by MiCA's rules regarding governance arrangements for CASPs and ART issuers, which explicitly reference DORA.¹¹⁶ However, the differing objectives of DORA and MiCA become apparent when considering whether CASPs are liable for failures in the underlying blockchain where their clients' crypto-assets are registered. Under MiCA, CASPs are liable for failures in permissioned blockchain networks, but not in permissionless networks over which they have no control.¹¹⁷ In contrast, DORA's objectives extend further, requiring financial entities to establish control through contractual relationships with their ICT third-party service providers. This includes infrastructure providers, as evidenced by DORA's specific targeting of cloud services.¹¹⁸ Therefore, CASPs and other financial entities in DeFi could potentially be held liable for entire blockchain networks under DORA. In terms of ICT services, DORA would be considered *lex specialis* to MiCA.

4. Centralised and decentralised provision of services

Contrary to the issuer and CASP concepts outlined in MiCA (see Part III.C.5 above), the definition of "ICT third-party service provider" does not differentiate between centralised and decentralised ICT services. This may seem surprising at first, but from a risk perspective it is irrelevant whether the ICT third-party service provider is a legal entity.

Nevertheless, some distinction between centralised and decentralised services is implied by the term "ICT third-party service provider", which refers to

¹¹⁴ See DORA, at Art 6(10), 19(5), 28(1)(a).

¹¹⁵ Traditional analogue telephone services are however exempted from DORA. See *Ibid* at Art 3(21).

¹¹⁶ See MiCA, at Art 34(10), 34(11), 68(7), 68(8).

¹¹⁷ According to the European Securities and Markets Authority's (ESMA) interpretation of Art 75(8) and Recital 83 MiCA. See European Securities and Markets Authority, *Technical Standards specifying certain requirements of Markets in Crypto Assets Regulation (MiCA) - second consultation paper* (Consultation Paper, ESMA75-453128700-438, 5 October 2023) at 19.

¹¹⁸ See DORA, at (20), (63). The explicit exemption of "traditional analogue telephone services" from the "ICT services" definition also indicates that other infrastructure services are covered by the definition. See *Ibid* at Art 3(21).

an “undertaking providing ICT services”.¹¹⁹ The term “undertaking” suggests that legal entity status is not necessary; when such status is required, the EU acquis uses the term “legal person”. However, the term “undertaking” is predicated on the existence of continuity and stable governance. In our view, we can apply the argument made earlier¹²⁰ regarding the distinction between centralised and decentralised applications: when an individual (such as a developer) or a group of individuals (eg, several developers) controls the DeFi application, it qualifies as an undertaking.

Because the regulated financial entity is responsible for both internal and out-sourced services,¹²¹ the key difference lies in the type of risk management rules applied. When a third-party service provider is involved, monitoring and risk assessment can concentrate on that specific provider, examining its setup and organisation as well as the potential impact of the provider’s default and technical failures on the financial entity, as outlined in Chapter V DORA. In the absence of a provider, the financial entity must address risks through its own risk management framework, in accordance with Chapter II DORA.

When applied to DeFi, a financial entity must ensure compliance with the ICT services outlined in Chapter V DORA that are delivered by different parts of the DeFi network, as long as there is someone controlling the application that qualifies as an ICT service from the financial institution’s perspective.¹²² However, if continuity, governance and control cannot be identified, the risk management rules under Chapter II DORA apply alongside sector-specific risk management requirements such as those under MiCA. In this scenario, a risk assessment of the service and business continuity measures will be necessary, and these measures must be developed and implemented by the financial entity without relying, either partially or fully, on the service provider.

This situation often highlights the significant risks associated with reliance on a truly decentralised service, as there may be no one responsible for the cybersecurity and business continuity essential for the ongoing provision or wind-down of the financial entity’s services when needed. Some exceptions exist for Bitcoin and Ether, which are archetypal fully decentralised cryptocurrency applications that have proven to be technically stable over time.

Nevertheless, the risk of depending on fully decentralised, uncontrolled applications remains with the financial entity under Chapter II DORA. This delineation encourages financial entities to favour applications that include a reliable service provider (*ie*, a control-holder) who can be held accountable and ensure business continuity when required. This approach aligns with DORA’s objectives, which stipulate that financial entities cannot ditch responsibility by using fully decentralised ICT services.

¹¹⁹ *Ibid* at Art 3(19).

¹²⁰ *Cf* MiCA at Art 19(1)(a), 59(1)(a); see Part III.C.5 above.

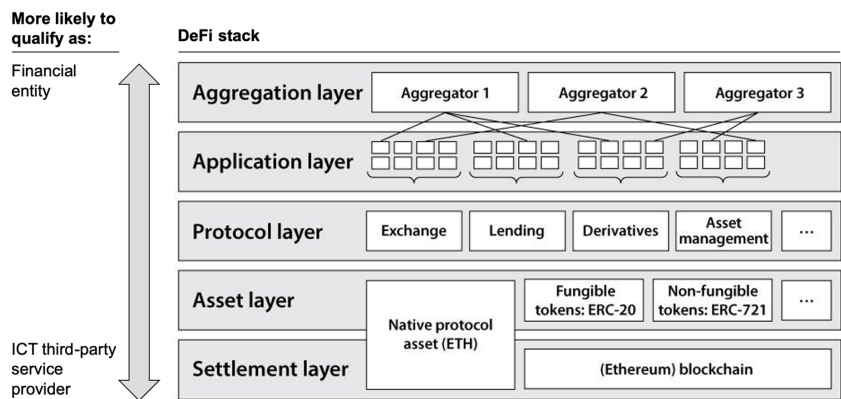
¹²¹ DORA, at Art 6(10), 19(5), 28(1)(a).

¹²² Zetzsche and Woxholth, *supra* note 3 at 262.

E. The Digital Operational Resilience Act in the DeFi Stack

In DeFi, the upper layers of the technology stack are inherently more customer-focused, while the lower layers are primarily technology-focused. As a result, entities operating at the higher layers are more inclined to provide financial services, whereas those at the lower layers are more likely to offer ICT services. In the context of DORA, this suggests that entities in the higher layers are more likely to be classified as financial entities, while those in the lower layers are typically considered their ICT third-party service providers. Although the reality is more complex, this straightforward categorisation serves as a useful reference for applying DORA to DeFi (see Figure 7).

Figure 7: The DeFi Stack



Source: Based on Schär, *supra* note 13 at 156. Modified by the authors.

The *aggregation and application layers* provide a user-friendly interface for delivering financial services to customers. Depending on how these services are provided, the providers of such applications and aggregation services may qualify as a financial entity under DORA, as an ICT third-party service provider for another financial entity, or both.¹²³ For example, they may qualify as “financial information service providers” under the forthcoming FIDA Regulation and thus be considered a financial entity under DORA.¹²⁴ Simultaneously, they might deliver ICT third-party services by offering their platform or user interface to financial entities further down the DeFi stack.

Specific challenges arise if applications or aggregators use the open data or application programming interfaces (“APIs”) of a financial entity without explicit agreement. In such cases, the financial entity risks becoming responsible for a third party of which it may not even be aware and with which it may not wish to interact. Whether the financial entity still receives an ICT service under DORA depends, in our view, on its business model. If such third-party applications and aggregators

¹²³ See *Ibid* at 264. On the situation where the same provider offers both financial and ICT services, see ch III.D.1 above.

¹²⁴ See FIDA at (32), Art 35.

play a significant role in delivering the underlying financial service, or if the financial entity has structured its data and APIs to facilitate these third-party applications and aggregators, it indicates reliance on ICT third-party services, even if no formal contract has been established with any service provider.

The **protocol layer** of the DeFi stack is complex, as it is where the actual financial services are created. Some entities within this layer may qualify as a financial entity under DORA, while others may solely provide ICT services and some may perform both roles simultaneously. This dual qualification as both an ICT third-party service provider and a financial entity is practically significant: they all offer “digital and data services” and qualify as an “ICT third-party service provider” if their services are utilised by another regulated financial entity. These services are often partially outsourced, such as through oracles that supply real-world data to the DeFi protocol. If such oracles are considered undertakings, and unless they qualify as a financial entity in this context, they qualify as ICT third-party service providers to a financial entity or offer data as subcontractors for an ICT third-party service provider.

The **asset layer** is where crypto-assets are created, typically using common standards. Entities like the Ethereum Foundation may act as ICT third-party service providers at the asset layer in certain cases where developers associated with the Foundation have established popular standards like ERC-20 and software tools to utilise them.¹²⁵ Issuers of crypto-assets and creators of smart contracts may also qualify as ICT third-party service providers if their utilisation of the underlying standards adds new code and functionality to the distributed ecosystem. The same holds true for software developers who create or maintain such software, unless they are classified as subcontractors; however, the regulated financial entity remains responsible for their services.

The **settlement layer** comprises the underlying digital infrastructure of DeFi, which we qualify as an ICT service. When provided by an undertaking, it constitutes an ICT third-party service provider. Various participants in a blockchain ecosystem may also qualify as undertakings providing parts of the settlement layer, such as software developers who develop and maintain the network code.¹²⁶ These participants qualify as ICT third-party service providers under DORA or as subcontractors to such a provider. The same likely applies to mining and similar activities of nodes within a blockchain network, which can be likened to conventional cloud computing and data centre services.¹²⁷ Because any “undertaking” may qualify as an ICT third-party service provider under DORA, the term potentially encompasses the entire ecosystem. Clearly, financial entities operating in DeFi networks risk being held responsible for a vast number of distant service providers.

¹²⁵ See Cointelegraph, “ERC-20 Inventor Discusses Origins, New Blockchains, BRC-20 and More” *Investing.com* <<https://www.investing.com/news/cryptocurrency-news/erc20-inventor-discusses-origins-new-blockchains-brc20-and-more-3135244>> (26 July 2023).

¹²⁶ See Zetzsche and Woxholth, *supra* note 3 at 263–264. On the Ethereum ecosystem, for instance, see Ethereum, “Welcome to the Ethereum Community Hub”, <<https://ethereum.org/community>>.

¹²⁷ Zetzsche and Woxholth, *supra* note 3 at 263.

In light of these challenges, we inquire how to ensure effectiveness of DORA-style risk management in DeFi in the next section, seeking to establish broad principles which may find further specification in future research.

IV. PRINCIPLES OF TECHNOLOGY RISK REGULATION FOR DeFi

The outset of DORA is sound: The prevalence of cyberattacks underscores the urgent need for enhanced cybersecurity in the financial sector. DORA offers a comprehensive, innovative, and essential regulatory response to the interconnected nature of the digital financial system and the potential systemic impacts of technology-related risks. As is often the case, the EU presents an innovative regulatory solution to a significant real-world issue, paving the way for the emergence of global standards. Key components of this framework include direct supervision of critical ICT third-party service providers and “pooled testing”, which may help level the playing field between large and small financial entities.

Furthermore, DORA’s focus on governance and continuous improvement, rather than prescriptive requirements, is a fitting approach to regulating innovation.

However, DORA is primarily designed with conventional finance in mind, which could have adverse effects on emerging financial concepts such as DeFi. As DeFi rapidly increases in volume and crypto-assets are increasingly recognised as US reserve assets, it becomes crucial to consider how to address DeFi-related technology risks more fundamentally.

In this section, while details must be left to future research, we develop three broad principles for regulating DeFi tech risks: (a) moving away from hierarchical concepts by adopting a network self-governance approach; (b) acknowledging the prevalence of smart contracts; and (c) aligning size-based exemptions among financial entities covered by the regulations.

A. From Hierarchy to Network Governance: The Plan of Operations

We do not contend that decentralisation alone justifies exemptions from financial laws.¹²⁸ In fact, the technology-related risks that DORA aims to address largely stem from the financial industry’s increasing reliance on digital technology, including complex interactions involving Big Data, AI, cloud computing and distributed ledger technologies (“ABCD”).¹²⁹ Nowhere is this reliance more pronounced than in DeFi, which seeks to disintermediate finance through technology.

However, any financial regulation that assumes a traditional hierarchy between a financial entity and its service provider, as seen in conventional finance, contradicts the horizontal design of DeFi. This horizontal framework often leads to large, complex and interconnected networks that span national borders, as illustrated in Figure 5 above. When regulators impose hierarchical structures on DeFi networks, every participant risks being held accountable for the compliance of all others.

¹²⁸ See Regulatory Challenges, *supra* note 27 at 115.

¹²⁹ See Buckley, Arner and Zetzsche, “Techrisk”, *supra* note 35 at 173 *et seq.*

This could result in widespread non-compliance among network participants, leading to a “tragedy of the commons”, where the absence of a coordinating entity leads to no improvement despite high regulatory costs.¹³⁰ These scenarios are difficult to reconcile with the foundational concept of accountable licence holders in conventional financial law and do not support the pro-innovation, “sentry at the gates” approach that regulators worldwide are striving to establish.¹³¹ To be effective, modern technology risk regulation must acknowledge the unique characteristics of DeFi.

To address this, lawmakers must clarify some form of hierarchy within these otherwise horizontal networks. We propose adopting a “Plan of Operations” approach.¹³² This approach is already embedded in another piece of EU financial legislation: Article 8 of the DLT Pilot Regulation, which grants regulatory privileges to DeFi experiments concerning the clearing and settlement of tokenised financial instruments.¹³³

Under the Plan of Operations approach, the financial supervisory authority can grant certain exemptions from mandatory financial laws to an operator who presents a plan of operations. This plan must include a governance structure for the peer-to-peer network that ensures compliance among all network participants.¹³⁴ Since the operator remains ultimately responsible for compliance, it has an incentive to promote adherence within the network. We anticipate that developer firms launching new networks will take on this role, ensuring that the code is designed to exclude participants who breach the conditions outlined in the plan of operations. While some may argue that such technical compliance contradicts the philosophy of “full decentralisation”, it effectively ensures adherence to overarching cybersecurity standards.

Over time, through experimentation with various plans of operations, both DeFi networks and regulators may establish more standard governance frameworks for horizontal networks that could ultimately be codified in law. DeFi may serve as a standard-setter as technology encourages conventional finance to adopt more network-based interactions. For instance, if traditional financial entities begin using online aggregators to reach customers, much like airlines and hotels do today, both the aggregators and the traditional financial entities could qualify as both financial entities and ICT third-party service providers in relation to one another.¹³⁵

¹³⁰ See on the tragedy of the commons as characteristic feature of decentralised finance, Zetzsche, Arner and Buckley, *supra* note 13 at 203.

¹³¹ Zetzsche and Woxholth, *supra* note 3 at 10.

¹³² Dirk A Zetzsche, Linn Anker-Sørensen, Maria Lucia Passador and Andreas Wehrli, “DLT-based Enhancement of Cross-border Payment Efficiency – a Legal and Regulatory Perspective” (2021) 15(1–2) *Law and Financial Markets Review* 70 at 103 *et seq.*; Dirk A Zetzsche and Jannik Woxholth, “The DLT Sandbox under the Pilot Regulation” (2022) 17 2 *CMLJ* 212 at 224–227 [Zetzsche and Woxholth, “DLT Sandbox”].

¹³³ Pilot regime for market infrastructures based on distributed ledger technology, EU Parliament and Council Regulation 2022/858, [2022] OJ L 151/1, <<https://eur-lex.europa.eu/eli/reg/2022/858/oj/eng>> (accessed 18 July 2026). On PilotR, see Zetzsche and Woxholth, “DLT Sandbox”, *supra* note 132; Zetzsche and Woxholth, *supra* note 3 at ch 12.

¹³⁴ Zetzsche and Woxholth, “DLT Sandbox”, *supra* note 132 at 224–227.

¹³⁵ New EU legislation, such as FIDA, may well further such business model innovations, thus transferring the DeFi-specific issues raised herein to other parts of the financial ecosystem. See FIDA at Art 35, (32), by which “financial information service providers” will qualify as financial entities under DORA.

B. *Recognition of Automated Contracting and Smart Contracts*

Whether or not smart contracts are used to coordinate DeFi networks, these networks are characterised by fluid, technology-enabled contracting. The mere act of executing a transaction can signify a contractual arrangement, with the specifics of such transaction-based contracts defined by software code.¹³⁶ This contrasts sharply with the legal requirements for conventional contracting procedures and terms. For instance, DORA mandates that contracts with ICT third-party service providers include written clauses concerning access, recovery and return of data, as well as specified rights and notice periods for contract termination.¹³⁷ In the case of ICT services that support critical or important functions, DORA also requires detailed exit strategies for each service provider.¹³⁸ Meanwhile, DeFi is designed with duplication of services across fluid networks, where the failure or exit of one node does not impact the network as a whole.

Any regulation addressing technology risk in DeFi must align legal arrangements with the realities of DeFi to prevent stifling potential ICT and financial innovation. This is particularly relevant given that the use of third-party services could provide an efficient pathway to new and innovative cybersecurity solutions.¹³⁹

To avoid unintended consequences, we suggest abandoning general rules on exit plans and contractual arrangements in favour of risk management clauses. These should focus on achieving effective risk management outcomes rather than dictating the specific methods for achieving them.¹⁴⁰ Alternatively, adopting a stricter definition of what constitutes an ICT service provider might have a similar effect, although this approach has its own drawbacks for cybersecurity. This situation highlights the need for a tailored set of implementing rules for DeFi and, ideally, a comprehensive re-evaluation of technology risk-related contracting requirements.

C. *Size-Based Exemptions*

The regulation of tech risks in DeFi must be crafted with the participants of the DeFi industry in mind. This necessitates a thoughtful approach to size-based exemptions. In particular, the regulation becomes excessive when any sole developer providing continuous software or server capacity is classified as an undertaking subject to technology risk regulation. DORA reflects this stringent approach, as the carve-out for small industry participants in Article 2(3) and 2(4) of DORA does not cover entities licensed under MiCA.

There are two perspectives regarding this strict application. First, one could view a strict scope as indicative of the interconnectedness of DeFi, which justifies increased scrutiny of tech risks, even under principles of regulatory proportionality.

¹³⁶ See Schär, *supra* note 13; J Woxholth, D.A. Zetzsche, R.P. Buckley, and D.W. Arner, “Competing Claims to Crypto-assets” (2023) 28 Unif L Rev 226, 236–237 with further references.

¹³⁷ DORA at Art 30(2)(d), 30(2)(h).

¹³⁸ *Ibid* at Art 30(3)(f).

¹³⁹ In the same vein, see Scott, *supra* note 15 at 24–26.

¹⁴⁰ *Cf* DORA, at Art 28(8).

This perspective considers interconnectedness a potential source of systemic risk; similarly, trading venues and central counterparties in traditional finance cannot qualify for exemptions from technology risk regulation, as they are the most interconnected financial entities.¹⁴¹ Alternatively, one might argue that including even the smallest tech developers in the regulatory scope is an unintended consequence of the regulation. Regulators lacking experience in crypto may struggle to delineate the nuanced boundaries required to adapt broad technology risk regulatory principles to the DeFi context.¹⁴² Consequently, the proportionality principle often found in modern technology risk regulation does not adequately account for the unique aspects of crypto.¹⁴³

If this is the case, we advocate for a purpose-oriented interpretation of technology risk regulation that considers the specificities of crypto and limits the scope to those nodes and developers that significantly influence and thus effectively rule and control the network's operations. As there cannot be two control holders at the same time, the control test suggested herein¹⁴⁴ would result in one entity, or a group of entities acting in concert with some steady organisation, being singled out as ICT service provider. Otherwise, regulators risk erring on the side of caution by imposing rules designed for the hierarchically structured traditional finance sector onto DeFi.

V. CONCLUSION

The intersection of DORA-style legislation with crypto and DeFi presents a policy dilemma, as legitimate cybersecurity and ultimately national security concerns clash with the innovation necessary for long-term digital and financial dominance. Solving this policy dilemma is indispensable for the effectiveness of DORA-style risk management in DeFi.

The rise in cyberattacks and digital operational failures indicates that, due to interconnectedness and potential systemic consequences, this issue cannot be left to the discretion of financial firms. DORA consolidates international best practices in technology risk management and positions the EU at the forefront of this field, potentially enhancing the Brussels Effect in the cyber domain.

However, we have outlined that this regulatory framework does not suit the most interconnected area within finance. While DORA mandates a hierarchical approach to ICT risk management, DeFi aims to achieve similar outcomes through horizontal financial infrastructures, distributing functions across numerous small participants

¹⁴¹ See for DORA's exemption for microenterprises, *Ibid* at Art 3(60).

¹⁴² We assume that this is the case in the EU, resulting in a state where crypto is the stepchild of DORA: given that MiCA had not yet been adopted when DORA was published in the official journal, the rules on MiCA were in many ways a *status nasciturus*. In turn, under the binding text, even small financial entities operating as part of DeFi networks must comply not just with sectoral cybersecurity measures, but also with the broad DORA requirements on incident identification, response, reporting, and learning, in addition to operational resilience testing and third-party risk management.

¹⁴³ See DORA at (7), (21), (39), (42), (64), (99), (105), Art 4, Art 7(a), Art 22(1), Art 28(1)(b).

¹⁴⁴ Regulators rely on existing concepts of corporate, securities and accounting law on control with modifications reflecting the different and often technical modes of control in DeFi.

linked by automated contracting. This highlights a fundamental challenge with the traditional approach to technology risk regulation in an innovative and globally interconnected sector, with wider implications for the ongoing efforts by global bodies to regulate the increasingly interconnected financial landscape.¹⁴⁵

To ensure the effectiveness of DORA-style risk management in DeFi, while preventing the undermining of DeFi and similarly innovative business models, we propose regulating along three principles broadly sketched out herein. These principles could provide the basis for a global standard for technology risk regulation in the highly international DeFi domain and possibly address the broader challenge of regulating innovation.

The principles include, first, that DeFi networks should define appropriate technology risk measures themselves provided these are outlined in a plan of operations supervised by financial authorities. Under this framework, an operator would be designated as the point of contact for compliance and enforcement concerning the DeFi network. Furthermore, automated contracting and smart contracts as well as size-based exemptions must be recognised and embedded in regulation. Under these conditions, the Plan of Operations approach reconciles advanced technology risk management with DeFi, accepting a moderate level of centralisation for a decentralised industry.

¹⁴⁵ See *eg*, Bank for International Settlements, “Project Raven” <https://www.bis.org/about/bisih/topics/cyber_security/raven.htm> (30 April 2024) (on AI and cybersecurity); Bank for International Settlements, “Project Leap”, <https://www.bis.org/about/bisih/topics/cyber_security/leap.htm>. Cyber resilience associated with third-party service providers is also explicitly featured in the CPMI work programme and strategic priorities for 2024–25, see Bank for International Settlements, “CPMI work programme and strategic priorities for 2025–27” <https://www.bis.org/cpmi/work_programme.htm>.