EUROPEAN CENTRAL BANK
EUROSYSTEM

Occasional Paper Series

Chryssa Papathanassiou

Digital innovation and banking regulation

No 351

Contents

Abstract

The European Union is aiming to foster digital transformation in all sectors by 2030. It has pioneered cross-sectoral legislation on artificial intelligence, cloud computing services and crypto-assets for this purpose. Yet compared with the work done on ESG, the prospective banking regulation regime has still to articulate more purposefully how the industry should manage the risks from digital trends and how supervisors should assess them. This paper discusses digital innovation in the banking sector in the context of the academic literature on financial innovation and non-banks. It also considers how to foster a risk-based Pillar 2 prudential framework, as well as market discipline through harmonised Pillar 3 disclosures. The paper concludes that these latter two propositions can help reconcile the challenges stemming from the short-term horizon applied in prudential assessment and the longer-term horizon over which digital innovation will take place in the banking sector.

Key words: digitalisation, artificial intelligence, crypto-assets, cloud computing, supervision

JEL: K 23, K 24

Non-technical summary

The Digital Finance Strategy sets out the European Union's commitment to fostering the digital transformation of companies by 2030. This paper discusses the interplay between three EU legal acts that implement this strategy and banking regulation.

The paper examines the digital transformation of European banks in the context of broader academic research into financial innovation and non-banks. The "dual nature of financial innovation" theory posits that cycles of prosperity arising from financial innovation are followed by cycles of severe disruption. The novel aspect with digital technologies is that any difficulty a bank may face can be disseminated instantly via social media, which has the potential to amplify its impact worldwide. The challenges are not new, but the question remains: how should digital innovation in the banking sector be regulated?

Some researchers advocate adaptive probing of banking regulation based on experience garnered from a short period of regulatory experimentation. The future Artificial Intelligence Act promotes this trend in the EU by means of regulatory sandboxes. These constitute a cultural shift in banking regulation, which is primarily rule-based.

Moreover, the phenomenon of re-intermediation follows the use of digital trends, with banks exiting certain market segments populated by new, technologically savvy, entrants.

The EU is encouraging digital trends by enacting an innovative framework. The Artificial Intelligence Act (AI Act)[1] will promote a level playing field for banks and non-banks as providers or deployers of AI systems. The Digital Operational Resilience Act (DORA)[2] strengthens cooperative oversight of critical cloud computing service providers by bringing together all relevant authorities, including prudential supervisors. The Markets in Crypto-Assets Regulation (MiCa)[3] is a dedicated and harmonised framework introducing a proportionate treatment of crypto-asset issuers and providers in a technology neutral way.

While the EU has pioneered a regulatory framework for digital trends, the banking package developed in parallel[4] remains largely agnostic, except for a few definitions.

---

1 On 21 May 2024, the Council approved the Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence e 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) (not yet published in the Official Journal).

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 (OJ L 333, 27.12.2022, p.1).

3 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (OJ L 150, 9.6.2023, p.40).

4 Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms (OJ L 176, 27.6.2013, p.1) and Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms (OJ L 176, 27.6.2013, p.338) (CRR III/CRD IV) (revisions not yet published in the Official Journal).

By contrast with the approach taken to ESG in the future CRR III and CRD VI, the banking regulation regime set out in CRR III and CRD VI does not articulate specific guidance on how banks should identify, monitor, evaluate and manage risks from digital trends, nor how supervisors should assess them. A review of the data currently provided by randomly selected significant institutions shows they are already disclosing information on their investments in and use of digital trends voluntarily, but not in a way that is comparable across peers.

Digital innovation will be a priority for European banks over the next decade, but this longer horizon needs to be reconciled with the shorter horizon used for prudential assessment, which typically spans one to five years. To meet this need, the paper suggests initiating digital innovation plans drawn up by banks for five years, but updated annually.

These would offer a comprehensive overview of all the risks to which a bank is exposed from various digital trends and allow for a risk-based Pillar 2 prudential assessment of how they might affect the business model, governance/risk management, capital and liquidity. At the same time, this paper suggests the EU could consider harmonising Pillar 3 disclosures so investors are able to assess the impact of digital innovation on the business model and profitability of large listed banks.

These two propositions call for concerted action on the part of supervisors, the EU and the EBA to adequately capture the risks and opportunities stemming from the digital innovation that is taking place in the banking sector.

1 Introduction

Banks are using digital trends to optimise customer experience and reap efficiency gains. The digital trends discussed in this paper include artificial intelligence (AI), crypto-assets and cloud computing services, which are all contemporary forms of financial innovation.

The Digital Finance Strategy sets out the EU's commitment to creating a safe environment for digital financial service providers and their customers by attaining four objectives by 2030: (i) remove fragmentation in the digital single market, (ii) adapt the regulatory framework to facilitate digital innovation, (iii) promote data-driven innovation by creating a common financial data space, and (iv) address the challenges and risks from digital transformation.[5]

In the past, financial innovation has often created a fragile equilibrium, with cycles of prosperity followed by severe failures. **To address the possibility of overreliance on digital innovation, this paper provides recommendations to shape a system of banking regulation that is fit for purpose.** The paper concludes that EU banking regulation should more purposefully reflect digital trends and the need for a state-of-the-art prudential and disclosure framework to promote the goal of adapting the regulatory framework to facilitate digital innovation.

This paper is structured as follows: Section 2 discusses the EU Digital Finance Strategy in light of the academic literature on financial innovation, non-banks and re-intermediation from new entrants in the value chain. Section 3 discusses how the EU is fostering digital trends in three specific regulations (the AI Act, MiCa and DORA). Section 4 discusses the limitations of the current banking regulatory framework when it comes to reflecting risks from digital trends. It further makes recommendations on how to foster effective Pillar 2 risk-based supervision, as well as Pillar 3 disclosures on banks' use of digital trends. The paper concludes that digital trends have the potential to revolutionise the way prudential supervision is performed, going beyond traditional off-site and on-site work and creating new forms of real-time embedded supervision.

5 See Digital Finance Strategy for the EU and 2030 Digital Compass: the European way for the Digital Decade. The Commission has expressed the ambition that by 2030 75% of European enterprises will have taken up cloud computing services, big data and Artificial Intelligence. See also FinTech Action plan: For a more competitive and innovative European financial sector.

2 The promises and perils of digital innovation

Banks are applying digital technologies to optimise customer experience and reap efficiency gains. The same logic has fostered all types of financial innovation throughout the ages. Yet, there is a duality in the nature of finance (Goetzmann, 2016), because innovations follow a recurrent cycle; phases of prosperity made possible thanks to technological advancements are followed by severe failures and financial collapse.

These failures have not been prevented in the past owing to regulatory capture and overreliance on the promises of innovation (Hellwig, 2009). Analysis of the 2008 financial crisis has shown the connection between increased demand for collateral in unregulated shadow banking markets and the financial innovation of securitised subprime mortgages (Gorton, 2010). The fact that shadow banking was allowed to blossom and compete with commercial banking without appropriate regulation and supervision was one of the root causes of the financial crisis.[6]

Metrick and Tarullo (2021) use the concept of "congruent regulation" of non-bank financial institutions to advocate similar regulation for similar risks to stability – irrespective of an entity's legal form or business model. Serious concerns surrounding data privacy have given rise to calls to democratise the private power behind "informational capitalism" (Kapczynski, 2020). New forms of technology can revolutionise how prudential supervision is performed. For example, distributed ledger technology (DLT) can make embedded supervision possible, allowing compliance of tokenised markets to be monitored automatically and transparently (Auer, 2019).

Better capitalised banks are a source of strength (Enria, 2022; Laeven et al., 2016). Yet it is equally true that serious flaws in financial system architecture greatly magnified the effects of the financial crisis, especially the procyclicality of capital requirements and the paradox of banking regulation (Hellwig, 2009). The latter means that minimum capital requirements are there to avoid a technical bank insolvency. Nevertheless, only capital held in excess of legal requirements may be available as reserves in a crisis.[7] Therefore capital measures alone cannot be the only response to any risks, including those from digital trends.

In view of the dual nature of financial innovation, regulatory experimentation with it is a mechanism for ascertaining which strategies might work best (Romano, 2018). Regulatory and supervisory innovation need to accompany financial innovation. Regulatory sandboxes are an example of a dynamic regulatory model based on

---

6 See *National Commission on the Causes of the Financial and Economic Crisis in the United States*, (2011), p. 255.

7 Hellwig (2009), p. 180. Regarding banks' propensity to use capital buffers and the impact of the regulatory capital relief measures implemented by the authorities during the pandemic, Couaillier et al. (2021).

adaptive probing: alternative strategies are tested in a legally safe environment (under waivers from existing regulations) and lessons learned feed into updating the regulation of financial innovations or training the next generation of supervisors (Allen, 2019).

As processes are unbundled, customers can choose and combine parts of the value chain from different vendors in an open finance model to achieve better pricing and customisation. This creates a new form of re-intermediation (Boot et al., 2020). New entrants include fintech firms.[8] These operate various models with limited or no regulation and can be active in different segments in the value chain. Fintechs are taking advantage of the growing demand for virtual finance and internet payments,[9] exploiting gaps in information analytics using multitemporal satellite change detection ("space added value") for risk management purposes[10] or bringing credit to the world's unbanked population.[11]

8 See the EBA website; also Communication from the Commission to the EU Parliament, the Council, the ECB, the European Economic and Social Committee and the Committee of the Regions, FinTech Action plan: For a more competitive and innovative European financial sector, COM/2018/0109 final.

9 For example WISE and Rocket Mortgage.

10 For example TELEKAIROS.

11 For example Prosperas.

3 The EU fosters digital trends

When the services sector in the EU was found lagging in digital trends in 2019,[12] the European Commission spearheaded the 2020 Digital Finance Strategy and pioneered legislation *inter alia* on AI, crypto-assets and cloud computing services that was unique worldwide.

The ten largest fintech firms in the world were located outside Europe.[13] The US comes top in the global ranking, followed by China and India, according to the 2021 Stanford Global AI Vibrancy Tool.

The digital transformation in the EU is already underway,[14] and is estimated to require investments of up to €1 trillion between 2020 and 2030.[15] The Digital Finance Strategy focuses on promoting use of cloud computing infrastructure, investments in software by adapting prudential rules on intangible assets[16] and uptake of AI tools.

3.1 A level playing field for providers and deployers of AI systems

A level playing field for all providers of AI systems

The first AI Act in the world will enter into force in 2024 and apply from 2025. Natural and legal persons providing and deploying AI systems are subject to a series of legal obligations (Article 16).

Consequently, the AI Act will create a level playing field among banks and non-banks which provide and/or use AI systems.[17] It creates three categories: high-risk AI systems are subject to a higher legal scrutiny; low-risk AI systems are subject to fewer obligations; unethical AI systems are prohibited. Member States must designate at least a national notifying authority and a national market surveillance authority as competent authorities (Article 59), which will exercise their powers to ensure application and implementation of the Act.

12 European Investment Bank (2019).

13 Barba Navaretti et al. (2020), p. 11. Fintechs were a supervisory priority of the Office of the Comptroller of the Currency for 2023.

14 Europe Central Bank (2018).

15 See European Commission (2020), Table 2.

16 Commission Delegated Regulation (EU) 2020/2176 of 12 November 2020 amending Delegated Regulation (EU) No 241/2014 as regards the deduction of software assets from Common Equity Tier 1 items (OJ L 433, 22.12.2020, p. 27).

17 The AI Act defines these as machine-based systems that are designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

A risk-based approach: AI systems for credit scoring are categorised as high-risk

One widespread use of AI in the financial sector relates to credit scoring, Upstart being an example.[18] Credit scoring systems are classified as high-risk AI systems (Article 6(2)). These are subject to a conformity assessment performed beforehand by the provider.[19]

Echoing Romano's adaptive probing, the EU advances regulatory sandboxes[20] for fintech and AI to promote innovation, and encourages national competent authorities to establish and operate them (Articles 57-59) to facilitate the safe development, testing and validation of innovative AI systems for a limited time before they are placed on the market or put into service pursuant to a specific plan under regulatory supervision.[21] The Artificial Intelligence Office[22] (Article 3 (47)) develops Union expertise and capabilities at the European Commission and contributes to the implementation of the AI Act.[23] The European Artificial Intelligence Board shall support the Commission to promote AI literacy and shall be composed of Member States representatives, a scientific panel and an advisory forum (recital 149).

Regulatory sandboxes need to be of limited duration not exceeding a few months, to address the concern that fintech firms or AI systems may shift into to a parallel world without appropriate regulation and supervision (Allen, 2019).

Since 2019 several supervisory authorities have set up innovation offices, strategic hubs for financial technology and regulatory sandboxes[24] to consolidate the lessons learned from the testing and piloting that takes place in sandboxes and assess innovative digital technologies from a risk-based perspective. In July 2023, the European Blockchain Regulatory Sandbox for cases involving DLT became operational and selected its first 20 cases across industries, the majority of which involve financial services and capital markets.

Banking supervisors should also consider using regulatory sandboxes to remain technologically up-to-date

Given the interest in AI tools for banking services, European banking supervisors will need to consider setting up regulatory sandboxes to ensure they remain technologically savvy about the risks and opportunities associated with supervised banks' use of digital trends.

---

18 Langenbucher and Corcoran (2021), p.16.

19 See Articles 19(2), and 43(2) AI Act; also Opinion of the European Central Bank of 29 December 2021 on a proposal for a regulation laying down harmonised rules on artificial intelligence (OJ C 115, 11.3.2022, p.5), para 2.2.5.

20 Council of the European Union (2020), para. 8; European Commission website; Allen (2022), p. 136..

21 Madiega and Van de Pol (2022).

22 Commission Decision of 24 January 2024 establishing the European Artificial Intelligence Office (C/2024/1459), OJ C 14.2.2024, pp. 1-5.

23 Articles 25(4), 53 and 56.

24 Cf. the CFPB disclosure sandbox in 2019; the SEC's FinHub since 2019; the OCC's innovation pilot program since 2019; the UK FCA's regulatory sandbox. See also the arguments for regulatory beaches where the supervisor has the position of a lifeguard instead of a partner sitting in the sandbox, Peirce (2018). An SSM-wide FinTech Hub was set up in 2017. See also the SSM Digitalisation Blueprint 2023-2028.

3.2 Cross-sectoral regulation of markets for crypto-assets

Several banks have invested in tokenised crypto-assets, but the collapse of algorithmic stablecoin TerraUSD in May 2022 showed both the magnitude of cryptocurrencies (Milne, 2022; FSB, 2022a) and their volatility (Gorton et al., 2022). MiCa introduced prudential, market conduct, and market abuse prevention rules for issuers and providers of crypto-assets[25] and asset-referenced tokens.[26]

This provides a worldwide paradigm of a proprietary regulatory framework which safeguards legal certainty concerning the issuance and trading of crypto-assets. By contrast, the SEC's power over digital tokens has been recently challenged in court in a suit that involves whether digital assets are classified as securities under US federal law.[27] MiCa was adopted after the BCBS developed the Pillar 1 treatment of crypto-asset exposures (BCBS, 2022) and while recommendations for crypto and digital asset markets were being finalised (IOSCO, 2023).

MiCa regulates the issuance and trading of crypto-assets and thus fosters legal certainty

MiCa regulates the issuing and trading of crypto-assets, which are categorised into three groups, and imposes prudential requirements commensurate to the risks associated with each of the three categories. Issuers of crypto-assets (other than asset-referenced tokens and e-money) admitted to trading are subject to a lighter regime, mainly consisting of publishing a white paper (equivalent to a prospectus).[28]

Issuers of asset-referenced tokens are subject to more stringent authorisation from designated competent authorities, including prudential requirements related to governance, own funds, reserve requirements and qualifying holding permissions.[29] The EBA is empowered to supervise those that it designates significant, with the help of a consultative supervisory college including ESMA and the ECB.[30]

Crypto-asset service providers authorised in the EU should have a registered office in the EU, ESMA maintains a register,[31] they are subject to prudential requirements and governance requirements,[32] and competent authorities are empowered to impose administrative penalties.[33] Significant crypto-asset service providers are supervised by the national competent authorities.

The EBA and ESMA, where appropriate in cooperation with each other and the ECB for credit institutions, are in the process of developing the requisite regulatory technical standards for them to exercise their new supervisory competence under MiCa.

---

25 A digital representation of a value or a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology.

26 A type of crypto-asset that is not an e-money token and that purports to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies.

27 SEC v Binance Holdings Ltd, 23-cv-01599, US District Court for the District of Columbia.

28 Article 5 MiCa.

29 Articles 34-36 MiCa.

30 Articles 117-138 MiCa.

31 Articles 109 MiCa.

32 Articles 67-68 MiCa.

33 Article 111 MiCa.

Given the global nature of crypto-asset activities, coordination between the EBA, national competent authorities, and prudential supervisors is necessary[34] to link banking regulatory requirements with those under MiCa (FSB, 2022).

Two important fields are excluded from the scope of MiCa. First, the Pillar 1 treatment of claims from digital assets; it is for the BCBS to lay out the treatment of tokenised claims on a bank and the criteria by which these may constitute deposits (BCBS, 2023). Second, MiCa does not regulate proprietary aspects (transfers and security rights) relating to crypto-assets; these are still subject to uncertainties and legal risk.

The UNIDROIT Principles on Digital Assets and Private Law offer a model for how to determine the applicable law concerning proprietary rights, custody, insolvency of a custodian or an issuer, and security rights for digital assets (UNIDROIT, 2023). Principle 5 is key; in principle, this provides that proprietary rights are governed by the domestic law specified by the issuer in the digital asset, or, failing that, the law specified in the system where the digital asset is recorded (party autonomy, deemed consent), or, failing that, the law of the statutory seat of the issuer.

This principle is designed to provide the incentive and freedom to the issuer of a digital asset to choose the law of its preference to govern the proprietary rights over digital assets.[35]

This principle may come to different results from the *lex rei/cartae sitae* rule applied in many European jurisdictions to determine the law governing proprietary rights to moveable and dematerialised assets. Thus, the EU may need to provide clarity in future in a legal act harmonising the conflicts of law regime for proprietary rights in digital assets.

3.3 Oversight of critical cloud computing service providers

Critical cloud computing service providers reportedly suffered major outages in 2021 and 2022.[36] With more data kept in the cloud, operational resilience is a serious concern. This was demonstrated when cyber threats and phishing increased during the pandemic[37] and during periods of geopolitical tension.[38]

The availability, security and integrity of data stored in a cloud computing provider, the risks of outages and data corruption, and access to data located in third countries are serious concerns for banks relying on these services. DORA addresses this new type of systemic risk posed by information and communication

---

34 Opinion of the European Central Bank of 19 February 2021 on a proposal for a regulation on Markets in Crypto-assets (OJ C 152, 29.4.2021, p.1), para 3.3.3.

35 Similarly, United States Bankruptcy Court Southern District of New York, in re: Celsius Network LLC, et al., Debtors, Memorandum opinion and order regarding ownership of Earn Account assets, Case No. 22-10964 (MG), 4 January 2023, p. 44. By contrast, in favour of proprietary rights over digital assets, see Arndt (2021).

36 Details here and here.

37 Hielkema (2022).

38 See the ECB website.

technologies (ICT) third-party service providers. Cloud computing service providers are characterised by criticality and a lack of substitutability. DORA follows a novel approach, expanding the concept of cooperative oversight known from financial market infrastructures to critical ICT third-party service providers.[39]

Strengthened oversight for cloud computing service providers which are critical for the financial system

The European Supervisory Authorities (ESAs) designate critical ICT third-party service providers for financial institutions, publish a list of them each year, and appoint one of the ESAs as the lead overseer. The lead overseer has investigative powers and may conduct on-site inspections and impose penalty payments and reporting obligations.[40] A similar approach was recommended in the US (Fratto and Reiners, 2019). ESA oversight will be financed by fees paid by the ICT third-party service providers.[41]

The ECB participates as an observer in the Oversight Forum that undertakes an annual assessment of oversight activities in relation to ICT third-party service providers and provides technical advice to the lead overseer on demand. The ESAs present an annual report to the European Parliament, the Council and the Commission on their oversight activities.[42] Prudential supervisors can provide valuable input for assessing concentration risk (Wuermeling, 2021). Professional secrecy requirements apply, so information may be disclosed only if foreseen under Union or national law.[43]

The use of cloud computing services varies across Member States, and concerns have been raised about the uncertainty over data location, geopolitical tensions and the dependency on key ICT third-party service providers to run essential services.[44] DORA addresses these worries by regulating the content of contractual arrangements with ICT third-party service providers. The contractual arrangements must include the locations where data is processed, the obligation to assist in the event of an ICT incident at no expense, the obligation to cooperate with competent authorities, termination and exit rights.[45]

A cooperative oversight framework for systemic digital service infrastructure is paramount for addressing the issues identified (Boot et al., 2020) and supervising services provided by so far non-regulated entities that are essential for banks. It utilises the experience with the successful example of SWIFT and CLS oversight (Crisanto et al., 2021). This regime is bold enough to institute strengthened oversight over facilities that are essential for the financial sector.

In comparison, the US Cloud Act imposes an obligation with extraterritorial effect on US companies holding data outside the US to report to the US authorities if legal

---

39 Article 3(23) DORA. Article 3(21) defines ICT services as “digital and data services provided through the 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”.

40 Articles 28, 33-44 DORA.

41 Article 43 DORA.

42 Article 32 DORA.

43 Article 55 DORA.

44 EBA (2019), para. 54(h); EBA (2017), para. 4.

45 Article 30(2)(b)-(i) DORA.

requirements are met.[46] Where banking organisations under the supervision of the Federal Reserve Board outsource core processing functions and are exposed to information technology-related risks, the responsible Reserve Bank may conduct information technology examinations of the service providers affiliated with the banking group.[47]

The definitions provided in DORA are reflected in CRR III and CRD VI, but without any further specification. If the EU is to attain its objective of facilitating digital innovation in the banking sector, it will be essential to link the banking regulation regime with the regulatory framework for the safe use of digital trends.

46 US v Microsoft Corp (Microsoft Ireland), No 17-2 (17 April 2018); Clarifying Lawful Oversees Use of Data (CLOUD) Act, H.R. 1625, 115th Congress, Division V.

47 See letter of February 29, 2000. A formal examination of an Amazon Inc. facility in Virginia was reportedly conducted in 2019. See also the guidance of the Federal Financial Institutions Examination Council to assist examiners; the OCC's risk management guidance; the Interagency Guidance on Third-Party Relations: Risk Management. Google Cloud and AWS explain how they address the respective regulations.

4 Banking regulation and digital trends

4.1 Gaps in banking regulation

Adoption of the final texts of CRD VI and CRR III is expected in the course of 2024. The new banking regime was mainly conceived to finalise implementation of Basel III, as well as introduce ESG aspects into Pillar 2 and Pillar 3 and harmonisation of supervisory powers. Regulation of digital assets has been developed in parallel. Thus, the upcoming banking package takes a minimalist approach to digital trends. It includes definitions of ICT risk from DORA and of crypto-assets from MiCa. Article 501d CRR III calls on the European Commission to assess, by June 2025, whether a dedicated prudential treatment of exposures to crypto-assets is justified, taking into account international standards (BCBS, 2023, Born et al. 2022).

Transparency of exposures within the perimeter of prudential consolidation

There is a need of transparency concerning risks from digital trends. Echoing Hellwig's proposal for transparency over the exposures of the whole system, the ESAs have advocated including all non-regulated entities that provide essential digital activities to banking or insurance groups within the perimeter of prudential consolidation (ESAs, 2022).

New impetus is provided by the updated Basel Core Principles for effective banking supervision (BCBS, 2024) which formulate the expectation that supervisors will monitor risks to banks from financial technology activities provided by non-bank financial intermediaries (NBFIs) belonging to a banking group. Supervisory powers and reporting should cover NBFIs within a banking group and any limitations will need to be remedied.

Nevertheless, the existing framework may not always enable authorities to request consolidation of all relevant non-financial entities of BigTech companies and other mixed activity groups (MAGs); a parent company must exceed the 50% threshold with respect to the financial services it provides to be classified as a financial holding company. As a consequence of the limitations of the current definitions, CRR III has new definitions of financial holding company (Article 4(1), new point 20) and ancillary services undertaking (Article 4(1), new point 18), while the provision of data processing and any other activity ancillary to banking has been added – but the 50% threshold still remains.

Enlarging the perimeter of consolidated supervision to capture fintech, AI, cloud computing service providers and BigTech parent companies or affiliates is one way of ensuring supervision. It is not a panacea, though, because non-financial affiliates require technically savvy supervisory expertise (Hakenes and Schnabel, 2014). Even if such firms were included in consolidated supervision, many tools such as early intervention measures and resolution tools are only available for banks, not non-banks and fintech firms (EBA, 2022), while the framework for supervision of financial conglomerates is unlikely to cover MAGs taking into account their core engagement with non-financial services (ESAs, 2022).

Linking the requirements laid down in the regulatory framework for digital trends with those provided in banking regulation

What is still missing is a detailed articulation of how banks will abide by the requirements in the AI Act, MiCa and DORA that links the obligations flowing from these acts with the obligations under CRR III/CRD VI. Ultimately, this involves providing guidance on how risks from digital trends should be captured and when quantitative or qualitative measures have to be applied.

Cooperation and information sharing between authorities to avoid duplication

The regulatory framework for digital trends attributes oversight and supervisory competences to national and EU supervisory authorities. This represents a dramatic change to the supervisory landscape. Close cooperation between prudential supervisory authorities and the competent authorities and lead overseers under MiCa, DORA and the AI Act will be essential to avoid regulatory arbitrage. Timely information is crucial when responding to cyberattacks or licensing crypto-asset providers,[48] because the technological challenges and opportunities are global. For non-bank providers, this entails cooperation between prudential supervisors and authorities which potentially may be outside the normal perimeter of banking supervision and financial stability. To allow for such a flow of information and to adapt to a fast-evolving world of supervisory architecture, the requisite framework for exchange of supervisory information may need to be adapted, in particular Articles 53-59 CRD. International cooperation is key for cross-pollination. Information Sharing and Analysis Centers (ISACs) are a practical example of informal international cooperation.

Digital innovation challenges the barriers between banks, regulated entities and other commercial entities whose services are essential for regulated ones. The upcoming banking regulatory regime needs to be updated to reflect the objectives of the Digital Finance Strategy and link with obligations under the AI Act, MiCa, and DORA. When the BCBS completes its work on Pillar 1 for crypto-assets, this will be implemented into EU law. The question that then arises is whether further reflection is required for Pillar 2 prudential assessment and Pillar 3 disclosures.

4.2 How to foster a risk-based prudential framework

On one hand, banks are required to hold capital and liquidity for the risks they face and demonstrate their capital or liquidity adequacy in ICAAP and ILAAP. On the other hand, they need to abide by the specific obligations in the newly enacted regulatory framework for digital trends.

For example, the use of credit scoring systems based on AI presupposes a conformity assessment with the AI Act performed by the provider, including documentation of various AI choices and limitations, the risks posed by the AI system and risk mitigation. The national competent authorities need to inform the ECB of their view of this assessment, so the latter can address the relevant risks in the SREP (recital 158 AI Act).

Another example is DORA which introduces obligations for all financial entities, including banks, to manage their ICT third-party risk (e.g. cloud computing service

[48] For banking supervision issues see ECB (2020), p. 28.

provider), keep registers of contractual arrangements and report new contractual arrangements with critical ICT third-party service providers to banking supervisors at least annually.[49] Banking supervisors will ensure banks comply with their DORA obligations. The lead overseer will inform the banking supervisor whether a critical ICT third-party service provider abides by the recommendations issued or not, and the banking supervisor will monitor whether banks properly account for the related ICT third-party risk.[50] Banking supervisors may adopt a decision which requires a bank to suspend or terminate the use of flawed critical ICT third-party services if the associated risks are not properly accounted for in the management of ICT third-party risk.[51]

Supervisors assess the capital and liquidity needs of banks in relation to their risks during the SREP, which is in principle an annual exercise; on this basis they may impose capital add-ons, provisioning, limits or other mitigating measures. The typical horizon of a supervisory review is one year, or in some cases up to five years, so there is a tension between the short termism embedded in the SREP and the long termism needed for digital innovation to be completed by 2030 and beyond.

In 2023 and 2022, it was acknowledged that banks face medium-term challenges and opportunities, such as the advance of digitalisation through the financial system. This requires closer scrutiny by supervisors, and the challenges from digital trends have to be prioritised.[52] Most risks from digital trends are not new: operational, reputational, concentration, market, credit, legal, and ICT risk.

Consequently, methodologies are necessary to assess and monitor the risks stemming from the use of high-risk AI systems, critical ICT third-party service providers and digital assets, and reporting templates need to be developed and aligned with existing ones.[53]

Digitalisation plans are suggested as a means of providing a comprehensive overview of all the risks from digital trends used by a bank

The supervisors will review banks' digitalisation strategies. It is hereby recommended that high-level strategies should be coupled with mandatory digital innovation plans offering a comprehensive overview of all the risks from digital trends to which a bank is exposed, and detailing how it assesses, manages, monitors and mitigates these. To provide a realistic quantification of the risks, digitalisation plans will need to be drafted looking at trends over the next five years and updated annually. Quantification of the risks stemming from digital trends is a novel front that deserves our attention. To ensure the necessary degree of proportionality, this obligation could be stipulated for large, listed banks.

New technologies implemented by banks and supervisors, such as DLT, open new gateways for delivering data to supervisors. Embedded supervision (Auer, 2022) would permit supervisors to automatically monitor supervised entities by reading the

49 Article 28 DORA.

50 Article 42(3), (4) and 6 DORA.

51 Article 46(a) DORA. ECB Banking Supervision is the competent authority for significant institutions.

52 See European Central Bank (2023), sections 5.1.3 and 6; also European Central Bank (2022), section 5.2.3 on the responsibilities of the management body and section 5.5.2 on operational resilience.

53 See Opinion of the European Central Bank of 4 June 2021 on a proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector (OJ C 343, 26.8.2021), p.1), para. 3.5.

supervised entity's ledger. The bank does not need to collect data and transmit them to supervisors, and the cost of compliance is therefore reduced. Consequently, digital innovation will likely change the way supervisors interact with the banks they supervise. This could eventually grow into a new concept that would transcend digital operational resilience: real-time supervision.

4.3 Market discipline through harmonised Pillar 3 disclosures

Voluntary bank disclosures concerning use of digital trends and strategies are already promising in terms of breadth, as Table 1 illustrates. Consistency of terms used and comparability across peers remain an issue, though, because some widely-used terms are not defined. A greater degree of convergence can be expected over the medium run as EU legislation implements universal definitions of terms and reporting templates, for instance for crypto-asset exposures (BCBS, 2023).

Pillar 3 disclosures regarding the use of digital trends may be considered

There is potential to streamline the quantitative and qualitative information disclosed by large, listed banks under Pillar 3. This would abide by the principle of proportionality. Pillar 3 disclosures would help investors determine the level of digital innovation and literacy in a bank, which can reveal a great deal about its business model and future profitability. The Pillar 3 ESG disclosure standards for large, listed banks provide a similar example, as well as the proposed disclosure requirements for crypto-asset exposures (BCBS 2023a).

If the European legislator decided to go down this road, an explicit legal basis would need to be incorporated in the CRR, and the EBA would provide guidelines and templates for disclosure.

5 Conclusion

The EU is fostering digital trends by means of an innovative comprehensive regulatory framework, including *inter alia* for AI systems, crypto-assets and cloud computing service providers. The interplay with the banking regulation regime could be reflected more purposefully in the regulatory framework. Digital innovation plans are suggested as a means of providing a comprehensive overview of all the risks to which a bank is exposed by using various types of digital trends. Consideration could also be given to harmonising Pillar 3 disclosures concerning banks' use of digital trends. Ultimately, digital trends have the potential to revolutionise the way prudential supervision is performed.

Table 1

Public information related to the use of digital trends by randomly selected banks

	Santander[54]	BNP Paribas[55]	Intesa[56]	Nordea
Investments	EUR 20 billion (2019-2022)	EUR 3 billion (2017-2020)	EUR 5 billion (2022-2025)	n/a
Users	54 million digital customers (2023) 54% of sales on digital channels (2022)[57]	280 million monthly connections to mobile apps on average (2022)	178 million transactions on mobile app (2023)	1 billion digital engagements per year (2022)[58]
AI	Yes[59]	Yes	Yes[60]	Yes[61]
Cloud	Optimised Hosting Environment (OHE)	Integrated Development Environment (IDE) with IBM	Project Skyrocket with Google	Db2 with IBM
Crypto-assets	In Argentina, to secure agricultural loans	Custody	n/a	n/a
DLT	Issued and redeemed blockchain bond	Issued digital bond[62]	Spunta Project, Marco Polo (R3)[63]	we.trade, Mercury[64]

Sources: Public materials accessed on 21 January 2024 and author's analysis.

54 Press release 7 March 2022; company website.

55 Press release 20 July 2022; company website, here and here; Press release 20 July 2022; company website.

56 Press release 26 January 2023; Pillar 3 disclosure 31 December 2023 and company website.

57 Company website and Financial Report January December 2023.

58 Company website; Press release 6 February 2023.

59 Company website.

60 Company website.

61 Annual Report 2023; Press release 29 March 2021.

62 Press release 12 July 2022.

63 Company website.

64 Company website.

6 References

Arndt, Johannes (2021), *Bitcoin-Eigentum*, Mohr Siebeck, Tübingen.

Assenmacher, Katrin et al. (2021), "A unified framework for CBDC design: remuneration, collateral haircuts and quantity constraints", *Working Paper Series*, No 2578, ECB, Frankfurt am Main, July.

Allen, Hilary J. (2019), "Regulatory sandboxes", *George Washington Law Review*, Vol. 87, pp. 580-645.

Auer, Raphel (2019), "Embedded supervision: how to build regulation into decentalised finance", *BIS Working Paper*, No 811, Bank for International Settlements, Basel, September.

Barba Navaretti, Giorgio, Calzolari, Giacomo and Pozzolo, Alberto (2020), "What are the wider supervisory implications of the Wirecard case?", European Parliament Economic Governance Support Unit, October.

Basel Committee on Banking Supervision (2024), "Core principles for effective banking supervision", consultative document, Bank for International Settlements, Basel, April.

Basel Committee on Banking Supervision (2023), "Cryptoasset standard amendments", consultative document, Bank for International Settlements, Basel, December.

Basel Committee on Banking Supervision (2023a), "Disclosure of cryptoasset exposures", consultative document, Bank for International Settlements, Basel, October.

Basel Committee on Banking Supervision (2022), "Prudential treatment of cryptoasset exposures", Bank for International Settlements, Basel, December.

Committee on Payments and Market Infrastructures: Markets Committee (2018), "Central bank digital currencies", Bank for International Settlements, Basel, March.

Boot, Arnoud et al. (2020), "Financial intermediation and technology: What's old, what's new?", *Working Paper Series*, No 2438, European Central Bank, Frankfurt am Main, July.

Born, Alexandra and Vendrell Simón, Josep M. (2022), "A deep dive into crypto financial risks: stablecoins, DeFi and climate transition risk," *Macroprudential Bulletin*, No 18, European Central Bank, Frankfurt am Main, July.

Couaillier, Cyril et al. (2021), "Bank capital buffers and lending in the euro area during the pandemic", *Financial Stability Review*, European Central Bank, Frankfurt am Main, November.

Crisanto Juan Carlos, Ehrentraud, Johannes and Fabian, Marcos (2021), "Big techs in finance: regulatory approaches and policy options", *FSI Briefs* No 12, Bank for International Settlements, Basel, March.

Enria, Andrea (2022), Interview with La Republica, 18 May.

EBA (2022), "Final report on response to the non-bank lending request from the Call for Advice on digital finance", Paris, April.

EBA (2017), "Recommendations on outsourcing to cloud providers", Paris, December.

EBA Banking Stakeholder Group (2021), "Own initiative Paper on Digitalisation: Challenges for consumers", Paris, December.

ECB Crypto-Assets Task Force (ECB 2020), "Stablecoins: implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the euro area", *Occasional Paper Series*, No 247, European Central Bank, Frankfurt am Main, September.

European Central Bank (2018), "Digitalisation and its impact on the economy: insights from a survey of large companies", *Economic Bulletin*, Issue 7.

Financial Stability Board (FSB 2022), "International Regulation of Crypto-Asset Activities. A proposed framework – questions for consultation", October.

Financial Stability Board (FSB 2022a), "Review of the FSB High-Level Recommendations of the Regulation, Supervision and Oversight of 'Global Stablecoin' Arrangements", Consultative Report, October.

Fratto, David and Reiners, Lee (2019), "A New Source of Systemic Risk: Cloud Service Providers", The FinReg Blog, 8 August.

Goetzmann, William N. (2016), *Money Changes Everything,* Princeton University Press, Princeton, NJ.

Gorton, Gary B. (2010), *Slapped by the Invisible Hand: The Panic of 2007*, Oxford University Press, New York, NY.

Gorton, Gary B., Ross, Chase P. and Ross, Sharon Y. (2022), "Making Money", NBER Working Paper 29710, National Bureau of Economic Research, Cambridge, MA, January.

Hakenes, Hendrik and Schnabel, Isabel (2014), "Regulatory capture by sophistication", University of Bonn, mimeo.

Hielkema, Petra (2022), "Supervision in a fast-paced digital world", speech given at the Afore Consulting 6th Annual FinTech and Regulation Conference, 9 February.

Hellwig, Martin (2009), "Systemic Risk in the Financial Sector: An Analysis of the Subprime-Mortgage Financial Crisis", *De Economist*, Vol. 157, No 2, pp. 129–207.

ESAs (2022), "Joint European Supervisory Authority response to the European Commission's February 2021 Call for Advice", EBA, EIOPA, ESMA, January.

International Organization of Securities Commissions (IOSCO 2023), "Policy Recommendations for Crypto and Digital Asset Markets", Final Report, November.

Kapczynski, Amy (2020), "The Law of Informational Capitalism", *Yale Law Journal*, Vol. 129, No. 5, pp. 1460-1515.

Langenbucher, Katja and Corcoran, Patrick (2021), "Responsible AI Credit Scoring – a Lesson from Upstart.com", in Avgouleas, E. and Marjosola, H. (eds.), Digital Finance in Europe: Law, Regulation, and Governance, De Gruyter, Berlin and Boston.

Laeven, Luc, Ratnovski, Lev and Tong, Hui, (2016), "Bank size, capital, and systemic risk: Some international evidence", *Journal of Banking & Finance*, Vol. 69 (S1), pp. S25-S34.

Metrick, Andrew and Tarullo, Daniel K. (2021), "Congruent Financial Regulation", BPEA Conference Drafts 25 March, The Brookings Institution, Washington, DC.

Milne, Alistair (2022), "Defining Digital Assets", SWIFT Institute Briefing Paper, April.

New York State Department of Financial Services (NYSDFS 2021), "Report on Apple Card Investigation", March.

OECD (2020), "Digital Disruption in Banking and its Impact on Competition", Paris.

Romano, Roberta (2018), "Pitfalls of Global Harmonization of Systemic Risk Regulation in a World of Financial Innovation", in Amer, Douglas W. et al. (eds.) *Systemic Risk in the Financial Sector: Ten Years After the Great Crash,* CIGI Press, Waterloo, ON.

Unidroit (2023), "Principles on Digital Assets and Private Law", Rome.

Wuermeling, Joachim (2021), "Exploring DORA - the Digital Operational Resilience Act and its impact on banks and their supervisors", speech given to the European Savings and Retail Banking Group (ESBG) virtually on 23 September.

Acknowledgements
The author thanks Andreas Beyer, Alberto Partida, Zaira Fernandez Ortiz, Georg Gruber, Prof. Hernany Veytia and the participants in the Banking Supervision Research Seminar for their useful comments on an earlier version of this manuscript.

Chryssa Papathanassiou
European Central Bank, Frankfurt am Main, Germany; email: chryssa.papathanassiou@ecb.europa.eu

PDF ISBN 978-92-899-6419-7, ISSN 1725-6534, doi:10.2866/137930, QB-AQ-24-015-EN-N