IN-DEPTH ANALYSIS

Requested by the ECON committee

European Parliament

Bigtech finance, the EU's growth model and global challenges

Economic Governance and EMU Scrutiny Unit (EGOV)
Directorate-General for Internal Policies
PE 755.724 - February 2024

EN

Bigtech finance, the EU's growth model and global challenges

Abstract

'Bigtech finance' – i.e. the provision of financial services by large digital conglomerates - has considerable implications for the EU's growth model and raises multiple regulatory concerns about financial stability; competition and market concentration; data protection; cybersecurity and operational resilience. Bigtechs also have potential geostrategic implications because the largest digital platforms are headquartered outside the EU. To address these global challenges, this study makes recommendations aimed at strengthening the regulation of Bigtech finance internationally and in the EU.

This document was provided/prepared by the Economic Governance and EMU Scrutiny Unit at the request of the ECON Committee.

This document was requested by the European Parliament's Committee on Economic and Monetary Affairs.

AUTHORS
Scott JAMES, King's College London
Lucia QUAGLIA, University of Bologna

ADMINISTRATOR RESPONSIBLE
Kai Gereon SPITZER

EDITORIAL ASSISTANT
Donella BOLDI

LINGUISTIC VERSIONS
Original: EN

ABOUT THE EDITOR
The Economic Governance and EMU Scrutiny Unit provides in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact Economic Governance and EMU Scrutiny Unit or to subscribe to its newsletter please write to:
Economic Governance and EMU Scrutiny Unit
European Parliament
B-1047 Brussels
E-mail: egov@ep.europa.eu

Manuscript completed in February 2024

This document and other supporting analyses are available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

DISCLAIMER AND COPYRIGHT

CONTENTS

LIST OF ABBREVIATIONS

BCBS	Basel Committee on Banking Supervision
BIS	Bank for International Settlement
ECB	European Central Bank
EU	European Union
FSB	Financial Stability Board
G7	Group of Seven
IMF	International Monetary Fund
IOSCO	International Organisation of Securities Commissions
UK	United Kingdom
US	United States

LIST OF FIGURES

EXECUTIVE SUMMARY

'Bigtechs' are large technology conglomerates that provide digital services. These digital platforms have expanded into the provision of financial services, mainly payments, but, increasingly, credit, insurance, asset management as well as experimenting with the development of private digital currencies.

Bigtech finance has considerable implications for the EU's growth model. It raises concerns for financial stability; competition and market concentration; data protection and data privacy; cybersecurity and operational resilience. Another concern is how to deal with the cross-border operations of Bigtech giants, which are headquartered outside the EU, but provide their services across the EU, as well as in third countries. Finally, the governance of Bigtechs is of critical importance to the EU's ambitions with regards to digital sovereignty.

The regulatory architecture for Bigtech finance is uneven: the EU has issued new rules, but international standards remain thin and siloed, while the main jurisdictions have adopted a patchwork of domestic regulatory approaches. This status quo is consequential because Bigtech finance is inherently cross-border and can develop quickly due to financial and technological innovation.

In light of the above, this study put forward the following recommendations:

1) To adopt a 'holistic' or 'hybrid' approach at the international level, complementing activity-based regulation in host countries with entity-based regulation in home countries.

2) To improve international cooperation between different sectoral regulators by establishing a high-level multi-sectoral regulatory forum bringing together financial regulators, competition authorities, data regulators and cyber-experts. In the first instance, this forum could be organised around the G7 countries. In the absence of the establishment of such as a forum, the EU should promote the creation of an International Digital Finance Network - modelled on the International Competition Network - composed of national and EU competent authorities with responsibilities covering different aspects of digital finance, including financial stability, investor protection, competition, data protection and cybersecurity.

3) To foster stronger bilateral cooperation over Bigtechs finance between the EU and US and between the EU and UK, as a precursor to international cooperation in multilateral fora.

4) Failing this, the EU could adopt an unilateralist approach, by issuing new EU rules in this domain first and then seeking to upload those rules to international fora, or cross-load them to third jurisdictions.

5) To improve cooperation between different sectoral regulators in the EU by establishing a multi-sectoral regulatory forum. This could be based on expanding the role of the High-Level Group established by the DMA – for example, by ensuring a more prominent role for central banks, and financial regulators. Initially, the scope of the EU level cross-sectoral body would be limited to knowledge development, information sharing, capacity.

6) The final recommendation concerns the facilitating role of the European Parliament.

1. WHAT IS BIGTECH FINANCE?

'Bigtech', a term that combines the words 'big' and 'technology', refers to large technology conglomerates that provide digital services - such as e-commerce, social media, and telecommunications - via digital platforms (Bains et al 2022; Crisanto et al 2021; Doerr et al, 2023), which combine digital and physical infrastructures to facilitate commercial, social and informational exchanges. Notable examples of Bigtechs include Apple, Google, Microsoft, Meta and Amazon in the United States (US), and Alibaba, Baidu, and Tencent in China. Bigtechs' business model rests on the 'data-network-activities' loop in that they collect a vast amount of user data, which are utilised to offer services that exploit network effects (meaning that the more people use a certain product or service, the more its value increases) generating further user activity. This loop is self-reinforcing because increased user activity then generates more data (BIS 2019).[1]

Over the past decade, Bigtechs have expanded into the provision of financial services via their digital platforms (hereafter in this paper, we refer to this phenomenon as 'Bigtech finance') – mainly payment services and e-commerce, but, increasingly, other forms of financial intermediation, such as credit provision, insurance, asset management as well as experimenting with the development of private digital currencies. Bigtech finance raises multiple regulatory concerns for the European Union (EU). These concerns have to do with systemic risk and financial stability; competition and market concentration; data protection and data privacy; cybersecurity and operational resilience. Bigtech finance also raises the issue for the EU of how to deal with the cross-border operations of Bigtech giants, which are headquartered outside the EU, but provide their services across the EU, as well as in third countries. Bigtech finance has considerable implications for the EU's growth model.

First, the provision of financial services by Bigtechs poses new challenges for financial stability, the functioning of the financial system, and its resilience to shocks, all of which can result in barriers to economic growth. Bigtechs' also pose risks for investor protection arising from greater market concentration, while the issuance of global stablecoins[2] by digital platforms could potentially impact the conduct of monetary policy. Second, the EU has mostly a bank-centric financial system, where banks traditionally provide funding to the real economy. The ability of Bigtechs that provide financial services to exploit multiple competitive advantages could encourage banks to engage in increasingly risky activities and could weaken banks' ability to provide credit to the real economy. Third, Bigtech finance raise concerns for data protection and, potentially, the use of those data for unfair market practices to the detriment of EU-based financial and nonfinancial companies, as well as their customers.

Fourth, cybersecurity is a condition *sine qua non* for the resilience of the financial system and individual firms therein. Bigtechs provide critical digital infrastructures (e.g. cloud services) to banks, insurers, asset managers etc and any disruption to these services could result in a 'critical event' for the financial system. Furthermore, if Bigtechs issue global stablecoins, they need to have adequate operational and cyber-resilience themselves. Fifth, Bigtechs are giant entities that operate across multiple jurisdictions with highly mobile activities, raising concerns about how to ensure adequate cross-border regulatory and supervisory cooperation. Finally, the governance of Bigtechs is of critical importance to the EU's

[1] Bigtechs are different from 'Fintechs', a term that comes from the merger of the words 'finance' and 'technology', which refers to financial firms that use digital technology and big data to offer new financial services, such as digital lending, digital banking, digital investment, blockchain payments and insurtech. Whereas Fintechs operate primarily in financial services, Bigtechs offer financial products as an extension of a broader set of business activities. Moreover, whereas traditional Fintechs unbundle financial services by separating traditional financial services (e.g banking) into smaller, specialized services that can be provided by different companies, Bigtechs re-bundle them, by selling several products or services together (Adrian 2021).

[2] 'Traditional' cryptocurrencies, such as Bitcoin, have experienced significant volatility as their value is not backed up by underlying assets. Stablecoins are private digital currencies (a.k.a cryptocurrencies) that hold a stable value relative to a specified class of assets, or a pool of assets. A global stablecoin has the potential to be used across multiple jurisdictions (EP 2021).

ambitions with regards to digital sovereignty given the geostrategic implications of the largest digital platforms being headquartered outside the EU.

It is important to note that this report focuses on the regulatory challenges posed by Bigtech finance for the EU and its economic growth, rather than providing a wider assessment of the advantages and disadvantages of digital finance more generally. One the one hand, platform finance could foster competition and market integration (e.g. by facilitating cross-border business) in financial services, potentially improving the quality of services, and reducing costs (Joint European Supervisory Authorities Report 2022). On the other hand, we would expect the focus of any future expansion of Bigtech financial services in the EU to be predominantly focused on credit provision to individuals and households, as existing bigtech customers, rather than large-scale lending for industrial or infrastructure development.

This paper is part of a broader academic research project undertaken by the authors on digital finance. The background material that fed into the preparation of that project has been gathered through the consultation of a variety of primary and secondary sources, and multiple confidential semi-structured elite interviews with policymakers and stakeholders within and outside the EU conducted during 2022 and 2023. This paper is organised as follows. Section 2 discusses the implications of Bigtech finance for the EU's growth model. Section 3 outlines the regulatory architecture for Bigtech finance in the EU and internationally. Section 4 spells out the main global challenges in regulating Bigtech finance in the EU. Section 5 puts forward some policy recommendations.

2. BIGTECH FINANCE AND THE EU'S GROWTH MODEL

The provision of financial services by Bigtechs has considerable implications for financial stability; market competition; data protection; cybersecurity and operational resilience. These issues are examined in turn.

2.1. Financial stability and investor protection

Bigtech finance raises multiple issues concerning financial stability. First, Bigtech finance is less stringently regulated than 'traditional' finance. In theory, most financial activities of Bigtechs fall within the existing perimeter of activity-specific financial regulation and those activities are regulated according to the principle 'same activity, same risk, same regulation' (IMF Borio 2021). For example, Bigtechs engaged in credit intermediation or offering payment services are regulated as non-bank lenders or payment firms and have to comply with rules on non-bank lending and payment services. Yet, Bigtech groups as a whole are not subject to entity-based prudential regulation (i.e. the rules designed to safeguard the financial resilience of individual entities as well as system-wide financial stability).

Whereas banking and insurance adopt an entity-based approach, other financial services are subject to an activity-based approach that targets the risks posed by the performance of specific activities (like payments or wealth management services). Accordingly, providers must hold licences to perform certain activities and are required to comply with specific operational standards. Activity-based regulation does not consider possible spillovers across several financial (and, non-financial) activities performed by a Bigtech group and the interlinkages between the financial (and, non-financial) entities in the group. A group-wide entity-based approach would enable the authorities to gather a comprehensive oversight of the groups' activities and the aggregate risk that they involve (Borio 2021; this point is elaborated further in Section 3).

The lack of entity-based regulation combined with the fragmentation of the regulatory architecture for Bigtech finance along sectoral lines and jurisdictional borders encourages regulatory arbitrage (meaning, the exploitation of regulatory gaps, loopholes, and overlaps) across activities and jurisdictions. To begin with, the traditional segmentation of the financial sector into banking, securities and insurance does not sit well with the business model of Bigtechs - the financial services they offer do not fit precisely into specific sectoral boundaries. Moreover, by making use of digital and financial innovations, Bigtechs can undertake certain financial activities in a manner that falls outside the existing perimeter of specific regulation, which could also affect investor protection.[3] Regulatory arbitrage could also involve other aspects of Bigtech's operations, such as data privacy and operational resilience (as elaborated below) (Bains et al. 2022). Cross-border regulatory arbitrage occurs if Bigtechs relocate their activities or their headquarters to jurisdictions that have less stringent regulation in place.

Furthermore, there are inherently financial stability risks associated with the systemic dimension of Bigtechs (Bains et al. 2022). Bigtechs have arguably become 'too-big-to-fail' institutions, owing to their size and systemic importance, mirroring the challenges posed by the largest global banks. Indeed, there are some significant similarities between 'big finance' and Bigtechs: size, interconnectedness and complexity (Foroohar, The Guardian, 8 November 2019). Even where the specific financial activities undertaken by Bigtechs may not be systemic in isolation, cumulatively they could generate significant financial risks (Adrian 2021) and could be scaled up relatively quickly. Moreover, Bigtechs and the

[3] The issue of investor protection is examined in depth by the joint response to the European Supervisory Authorities to the European Commission's February 2021 Call for Advice on digital finance and related issues.

financial services they offer are deeply interconnected with the 'traditional' parts of the financial sector as well as with other parts of the economy. In fact, Bigtechs have developed into critical financial infrastructures operating outside the traditional financial system, but strictly interconnected with it, as well as through the provision of critical third-party services, such as cloud storage (Crisanto et al. 2022). These services are highly concentrated. The failure of just one large digital platform would create a 'significant event' in the financial system, rendering Bigtechs 'too critical to fail', Adrian 2021) (this point is developed further below, when discussing Bigtech and cybersecurity).

Third, Bigtechs have significant potential to expand the issuance and usage of global stablecoins. Over the last decade or so, crypto-assets and crypto-currencies (notably, stablecoins), have increased due to advances in technology, financial innovation and decentralised finance. At the same time, Bigtechs have begun to provide financial services. The intersection of these two trends means that whereas stablecoins have had limited uptake so far. Yet, stablecoins could experience a leap forward at the global if issued by Bigtechsby leveraging the large users' base and network externalities of Bigtechs (Panetta 2021). Thus, stablecoins issued by Bigtech could rapidly become global stablecoins, and be used as a digital alternative to 'traditional' money, affecting the conduct of monetary policy, in particular, the credit channels of monetary policy. Furthermore, in order to keep their value constant, stablecoins are generally backed by high-quality liquid assets. The issuers of stablecoins then compete with banks and other financial companies for access to those kinds of financial assets. Banks' funding conditions could become more expensive if depositors switched from traditional bank deposits to deposits held by large stablecoin issuers. Banks' funding conditions could also become more volatile as the amounts of assets managed by stablecoins increase. In extreme circumstances, a run on a global stablecoin could trigger financial contagion through the liquidation of the underlying assets to cover redemptions (Panetta 2021). Beside concerns related to financial stability, stablecoins raise important issues for investor protection (for instance, the right to seek recourse for unauthorized transactions), data protection (data gathering and data sharing), cybersecurity and operational resilience (EP 2021). Finally, stablecoins can become a vehicle for money laundering and the financing of illegal activities, as well as facilitating cybercrime, tax evasion and tax avoidance. They could also be used to circumvent economic and financial sanctions and capital controls. This is because the anonymity that stablecoins guarantee makes it difficult for the public authorities to monitor transactions and beneficiaries (Bains et al. 2022b).

Bigtech's issuance of global stablecoins feeds into the broader debate on digital currencies, which, in turn, intersects with the discussion concerning the issuing of central bank digital currencies (Angeloni 2023), as an alternative to private digital currencies (EP 2021). In fact, digital transformations and the expansion of digital finance raise the issue of whether central banks should provide digital currencies and according to which parameters. In the EU, to be precise, the euro area, the European Central Bank (ECB), has shifted from initial lukewarm support concerning the prospect of issuing its digital currency to taking a leading role (ECB 2023; Panetta 2022a, 2023), jointly with the European Commission (2023), in paving the way for the introduction of a digital euro (see also Euroarea summit 2021). The ECB has also been involved in policy discussions taking place on this matter at the international level, notably, in the Bank for International Settlements (BIS), the Financial Stability Board (FSB) as well as the Group of Seven (G7) finance ministers and central bank governors. Several factors account for the ECB's support for a digital euro, unlike, for example, the Federal Reserve, which has remained sceptical about central bank digital currencies (for example, Waller (2021) referred to central bank digital currencies as 'a solution in search of a problem').[4] To begin with, the ECB and some other central banks are concerned about the potential upscaling of private digital money, which would impact the conduct of monetary

[4] This was also the title of a House of Lords (2021) inquiry on central bank digital currencies.

policy and the stability of the financial sector. Moreover, the ECB and the European Commission are sponsoring a digital euro for geopolitical reasons, including to safeguard the 'monetary sovereignty' of the euro area, the deployment of the digital euro as a 'soft power' tool, and the promotion of the international usage of the euro with a view to underpinning it as a leading international currency (Euro area summit 2021).

2.2. Market Competition

The provision of financial services by Bigtechs has important implications for market competition and market contestability due to the capacity of Bigtechs to challenge the position of established financial services providers (first and foremost, banks) in several ways. First, digital platforms Bigtechs can use their large customer base, access to data, and network advantages to establish 'platform banks' providing a range of financial services – from payments to deposits, credit provision and wealth management (Stulz 2019). Thus, Bigtechs can exploit regulatory arbitrage arising from the 'blurring of boundaries' between finance and social media, and the use of different tools and interfaces by Bigtech firms. All this could lead to excessive concentration and anti-competitive practices, such as cross-subsidisation, or giving preferential treatment to their services (Crisanto et al. 2021). It could stifle market competition and trigger abuse of market power. [5]

Second, the absence of entity-based regulation for Bigtechs gives them competitive advantages over traditional financial companies, which are subject to activity-based regulation as well as entity-based regulation. Since Bigtechs benefit from a less comprehensive regulatory framework, the 'same activity, same risk' approach creates an uneven playing field between Bigtechs and financial incumbents (first and foremost, banks). Thus, digital conglomerates are able to provide many financial services at a lower cost than traditional banks, which are subject to more stringent rules (Bains et al 2022; Stulz 2019). Furthermore, some provisions, such as Open Banking, which were initially designed to foster competition between banks and non-bank companies offering financial services, had unintended effects, allowing Bigtechs to gain access to and thus benefit from a large amount of data that banks had collected, without being subject to reciprocal obligations, that is to say, without having to provide some of their customers data to banks (Gambacorta et al. 2022). Competition between Bigtechs and banks is consequential for the EU's economy, which has mostly a bank-centric financial system where banks provide the bulk of funding to the real economy, especially to Small and Medium Enterprises.

To be sure, the relationship between digital platforms and banks is complex. Many banks view the provision of financial services by Bigtechs as a competitive threat owing to their ability to exploit economies of scale and network effects (Hendrikse et al. 2019). This is compounded by a regulatory regime that is seen as favourable for Bigtech challengers (Gambacorta et al. 2022). Yet, banks sometimes cooperate with Bigtechs in providing financial services. In fact, while some Bigtechs have expanded payment services by 'disintermediating' traditional finance, others opted to partner with banks. Furthermore, banks and Bigtechs are increasingly entangled through the diffusion of digital technology. Indeed, banks are increasingly adopting the platform business model for themselves through partnerships, investments and acquisitions of fintech firms (Langley and Leyshon 2021: 380). In addition, financial institutions are highly dependent on Bigtechs for critical digital infrastructures, such as cloud services and application softwares. The result is a complex ecosystem of relationships defined by logics of collaboration, adaptation and competition (Macartney et al. 2022).

[5] Bigtechs raise broader issues concerning competition and market contestability outside the financial sector that we do not discuss in this paper.

2.3. Data Protection

The provision of financial services by Bigtechs has important implications for data privacy in general and (sensitive) financial data in particular, as discussed briefly above. The ability to gather, store and use consumer data is core to the business model of Bigtechs, giving them a competitive edge on competitors. Furthermore, the availability of large quantities of data increases the risk that data correlated with race or gender could be used in a discriminatory way, for instance, in making decisions about lending, thus de facto resulting in a form of 'algorithmic discrimination' (Doerr et al. 2023). In addition, platform infrastructures' access to personal data permits the harnessing of those data to manipulate behaviour, or to engage in forms of digital surveillance (Campbell-Verduyn and Lenglet 2022). Data privacy and data protection are particularly important in the EU, where the General Data Protection Regulation set in place the world's most comprehensive 'rights-based' approach to date, prescribing, inter alia, 'data localisation', whereby platforms are required to store and process citizens' data in the country of origin, with strict rules covering international data transfers. By contrast, the US and China, where the Bigtechs are based, have less stringent data protection rules (Carstens 2019).[6]

2.4. Cyber-security

The provision of financial services by Bigtechs has important implications for cybersecurity, which covers a range of issues, from operational resilience to cybercrime. The most immediate risk stems from the dependency of financial and non-financial companies on critical third-party services provided by Bigtechs, such as cloud storage. Over the last decade or so, financial institutions have moved critical operations, such as online banking and payment services, to the cloud, operated by the Bigtechs. Since market concentration in the provision of cloud services is very high, disruption to services involving a single digital platform could bring down key financial services across multiple banks and countries. That would leave customers unable to access services, undermining confidence in the financial system, and potentially triggering a wider market shock (Withers and Jones 2021). It is therefore necessary to improve operational resilience, ensuring that institutions can still function in the event of serious disruptions, including cyber-attacks, and have robust contingency plans in place (Crisanto et al 2022). Yet, financial regulators and the financial companies they supervise have limited understanding of cyber security and generally have limited access to relevant Bigtechs information and data because these companies are not within the purview of financial regulators. In response, financial regulators, like competition and data protection authorities, call for more powers for them to scrutinise the activities of the digital giants).[7] Cybersecurity is also important for the development of stablecoins, cryptocurrencies and crypto assets. Cybersecurity and operational resilience are particularly consequential for the EU, whose financial and non-financial companies (as well as public utilities and state administrations) rely on the digital services provided by Bigtechs located outside the EU. The EU has taken steps with reference to the cybersecurity and operational resilience of financial companies, as discussed below.

[6] The General Data Protection Regulation allocates rights on data to individuals. In the USA, fragmented sector-specific data regulation means that, in practice, companies have relatively free access to the data of individuals (Boissay et al. 2021)

[7] Joint European Supervisory Authority (2022) Response to the European Commission's Call for Advice on digital finance and related issues, 31 January. Panetta (2021). Panetta, F. (2022b) 'For a few cryptos more: the Wild West of crypto finance', 25 April. Euractive (2022) 'Scant resources might threaten enforcement on Big Tech, EU data protection bodies warn', 13 September.

2.5. Geopolitics

Finally, the provision of financial services by Bigtechs has geopolitical consequences because the largest digital platforms are all based outside the EU. As critical infrastructures for increasing swathes of economic activity, states that host the largest Bigtech firms – namely, the US and China – actively seek to cultivate and direct digital platforms for their own geoeconomic and geopolitical ends. This new 'state platform capitalism' (Rolf and Schindler 2023) constitutes a form of extraterritorial power through which jurisdictions compete to recruit overseas users to rival state-platform nexuses as a means of integrating countries into respective spheres of influence (van Dijck and Lin 2022). For the EU, dependency on overseas digital platforms is increasingly perceived as a geopolitical vulnerability (Amoore 2018). While the EU has in recent years adopted a more proactive approach to supporting the development of domestic digital platforms, the continued reliance on predominantly US-based bigtechs for critical services and infrastructure constrains the EU's ambitions regarding the need for greater 'digital sovereignty' and 'open strategic autonomy' (Broeders et al. 2023).

3. THE REGULATORY ARCHITECTURE FOR BIGTECH FINANCE

The regulatory architecture for Bigtech finance is uneven: the EU has issued new rules over the last few years, but international standards remain thin and siloed, while the main jurisdictions have adopted a patchwork of domestic regulatory approaches. This status quo is consequential because Bigtech finance is inherently cross-border and can develop quickly due to financial and technological innovation..

3.1. The recent developments of the EU's regulatory framework

The EU has been a 'first mover' worldwide in regulating Bigtechs. In 2022-2023, it passed the Digital Services package, which contained several pieces of legislation: the Digital Services Act, the Digital Markets Act, the Digital Operational Resilience Act, and the Markets in Crypto-Assets Regulation. The purpose of EU rules was manyfold, besides regulating Bigtech's provision of financial services in the EU. In fact, the additional aims the Digital Services package were for the EU to act as a first mover globally in regulating this field, as well as 'creating a climate that is more conducive to the emergence of European players in the technological field' (Villeroy de Galhau 2023).

The Digital Services Act sets new obligations for online intermediaries, depending on their role, size and impact in the online ecosystem. All online intermediaries offering their services in the EU are required to comply with the Act, which creates a public oversight of online platforms that are used by more than 10% of the EU's population.[8] The Digital Markets Act establishes criteria for designating large digital platforms as 'gatekeepers' that are subject to new ex-ante obligations.[9] Specifically, gatekeepers are required to allow third parties to inter-operate with the gatekeeper's own services, allow their business users to access the data that they generated by using digital platforms, and allow their business users to conclude contracts outside the gatekeeper's platform. Gatekeepers are also prohibited from treating services and products offered by the gatekeeper itself more favourably in ranking than similar services or products offered by third parties on the gatekeeper's platform and prevent consumers from linking up to businesses outside their platforms.[10]

[8] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en
[9] The Commission is to decide which companies qualified as gatekeepers, according to set criteria and was given the powers to conduct investigations for misconduct or non-compliance with the Digital markets Act rules.
[10] https://digital-markets-act.ec.europa.eu/index_en

In the area of operational resilience, the Digital Operational Resilience Act sets EU requirements for the digital security of companies operating in the financial sector as well as critical third parties that provided information and communication technologies to them, such as cloud platforms or data analytics. It was intended to mitigate cyber threats and enhance digital operational resilience, by establishing specific requirements on critical third-party providers.[11] It adopted an activity-based approach mandating all financial institutions to create robust risk and crisis management frameworks, and established direct EU-level oversight for 'critical' service providers (ENISA 2021). Thus, the EU has mitigated the concentration of cloud service providers by imposing requirements on the financial companies that use those services (Adrian 2021).

The Markets in Crypto-Assets Regulation covered crypto assets[12] previously not regulated by other EU financial services legislation. This piece of EU legislation set requirements for issuers of crypto-assets in the EU and crypto-asset service providers wishing to apply for authorisation to provide their services in the single market. It set transparency, disclosure, authorisation and supervisory rules for the issuing and trading of crypto-assets, including stablecoins. It prescribed capital and liquidity requirements, rules on the custody of assets as well as rights of the investor against the issuer. Issuers of significant asset-backed crypto-assets were to be subject to more stringent capital and liquidity requirements, as well as interoperability requirements. The EU has been a 'first mover' worldwide in regulating crypto-assets and the broader 'crypto' environment. As explained next, international rules (i.e. soft law) on these matters are very underdeveloped.

3.2. The Thin and Siloed Financial Architecture

The international regulatory architecture for Bigtech finance is thin and siloed. In fact, this matter is discussed in a piecemeal way by a variety of sectoral standard-setters – there is no designated 'go to' body or even one taking the lead in orchestrating the work of other bodies. To date, international standards[13] for Bigtech finance have not been proposed and the activities of international standard-setting bodies that bring together domestic regulators from various jurisdictions have been limited to research with diagnostic scope and minimal declaratory statements. The International Monetary Fund (IMF) and the Bank for International Settlement (BIS) have been particularly active in mapping the contours of this emergent regulatory field and seeking to facilitate cross-border cooperation, for instance by publishing regular reports detailing the systemic risks posed by platform finance, developing shared metrics for measurement and analysis, and proposing and evaluating different regulatory solutions. Their accumulation of considerable technical expertise has enabled these bodies to advocate more stringent regulation of Bigtechs in recent years (James and Quaglia 2024).

For example, the IMF has likened Bigtech finance to shadow banking (Adrian 2021), arguing that 'both have grown outside the regulatory perimeters to have potential systemic implications' and that certain entities and activities of both shadow banking and BigTechs ecosystems can relatively easily relocate to jurisdictions where regulations are less stringent. The IMF has called for 'broader coordination with nonfinancial regulators and competition authorities' to 'mitigate risks to financial stability, market integrity, and consumer protection' (Bains et al. 2022). Like for shadow banking, it has advocated 'a hybrid approach, combining a mix of entity- and activity-based approaches' for Bigtech finance.

[11] https://www.digital-operational-resilience-act.com/

[12] Crypto-assets are sector digital assets that rely on cryptography and distributed ledger technology. The different types of crypto-assets include unbacked crypto-assets (such as Bitcoin), backed crypto assets (so-called "stablecoins"), see https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/crypto-assets-and-global-stablecoins/

[13] International standards usually take the form of 'soft law', which is not legally binding, but the expectation is that jurisdictions that sign up to/agree to certain international standards will then implement them domestically.

The BIS (2019), like the IMF, has stressed the potential impact of Bigtech finance on financial stability, noting that the existing regulatory approach was not designed for Bigtechs and therefore does not deal with the potential negative 'spillovers' across their activities and their potential systemic relevance. The BIS has criticised the existing 'silos-like' regulation, stressing instead the need for cross-sectoral and cross-border cooperation (Boissay et al. 2021). More recently, the BIS has called for a shift from 'activity-based' rules to 'entity-based' rules, concluding that international standards are necessary for a consistent policy response worldwide (Carstens 2023) (this matter is discussed further in the penultimate section).

The Financial Stability Board (FSB) has explored the financial stability risks related to Bigtech finance (2019, 2020) and the dependencies of financial companies on cloud services provided by Bigtechs. The FSB (2023a,b) has also done some work on crypto assets, stablecoins and central bank digital currencies. Yet, on these matters, the FSB has issued some 'high level' principles that are rather general so as to be applicable across very different jurisdictions (thus, they lack precision and stringency). At a more practical level, FSB has developed a common handbook of cybersecurity terminology based on existing ISO and US cyber security standards, the 'Cyber Lexicon' (FSB 2018). The FSB generally has a coordinating role in orchestrating the work of sectoral international standards setters in finance (e.g the BCBS, the IOSCO), which are also members of the FSB, but it has been constrained from taking a more active role on Bigtech finance due to disagreements among member jurisdictions and internal tensions between a variety of sectoral financial regulators. These points are elaborated next.

Interstate competition has inhibited the development of international standards for Bigtech finance by the FSB and other international standard-setting bodies in finance. The largest home jurisdictions for global bigtechs firms, the US and China, have been proactive in promoting the growth, competitiveness and international reach of their domestic platforms, and are keen to avoid bearing the cost of having to adjust their domestic regulatory frameworks to new global rules. Whereas in some other areas of financial regulation the US have acted as 'pace-setters', prompting international standard setting, for instance, on banking and derivatives (Quaglia 2014), that has not been the case for bigtech finance, as suggested by several interviews conducted for an academic study on this matter (James and Quaglia 2023). Conversely, the EU has long been the chief proponent of international standards to address cross-border externalities generated by third-country Bigtechs, but also to support the development of European digital competitors (James and Quaglia 2023). In recent years, the international policy discussions have been slowed down by increasing geopolitical tensions between the US and China over the use of digital technology, the production of semiconductors, and fears over cyber and national security, culminating in the imposition of economic sanctions by the US and China.

Furthermore, the possibility of developing new global rules remains constrained by the absence of a single international body with overarching responsibility for Bigtech finance. This is in part because it is a new area of regulation that intersects a variety of policy areas, including financial services, market competition, data protection, and cybersecurity. Even within the policy area of finance, there are several international standard-setting bodies that bring together domestic sectoral regulators that have divergent mandates, objectives and regulatory approaches, including monitoring the building up of macroprudential risk and safeguarding system-wide stability (the FSB); the risk management and financial resilience of regulated entities (i.e. banks) (the Basel Committee on Banking Supervision, the BCBS); investor protection and (securities) market integrity (the International Organisation of Securities Commission, the IOSCO); and resilience of market infrastructures (CPMI) (Quaglia 2022). International standard setting bodies in finance sit in the FSB, but that is insufficient for meaningful cooperation in new policy areas that have far reaching implications, such as digital finance. The rifts among financial

regulators are intensified by the involvement of a range of other regulatory agencies – notably those concerned with data privacy, telecoms infrastructure, and cybersecurity – that have different mandates and regulatory approaches (James and Quaglia 2023). This regulatory fragmentation generates obstacles to international cooperation.

In the field of competition policy, the International Competition Network brings together national and multinational competition authorities. It is an informal venue to foster regular dialogue and promote the convergence towards sound competition policy principles worldwide. The International Competition Network does not have any rule-making function. However, it issues by consensus recommendations, or "best practices," and it is then up to individual competition authorities to decide whether and how to implement the recommendations domestically.[14] In the field of data protection, the Global Privacy Assembly brings together more than 130 data protection and privacy authorities from a variety of jurisdictions. One of the main aims of the Global Privacy Assembly is to foster regulatory dialogue among its members and cross-border cooperation, also for enforcement.[15] In the field of cybersecurity, the Cyber Expert Group was established by the Group of Seven (G7) to build confidence, foster trust and share knowledge about operational resilience and cyber risks. The group has relied on financial institutions to report cyber incidents and responses to assist learning and adaptation among other Cyber Expert Group members.

[14] https://www.internationalcompetitionnetwork.org/about/
[15] https://globalprivacyassembly.org/enforcement-cooperation-repository/

4. BIGTECH FINANCE IN THE EU AND GLOBAL CHALLENGES

Bigtech finance poses global challenges for the EU. To begin with, it is a relatively new issue and therefore an 'emergent field' of regulation. Relevant data are still in the process of being gathered and subject-specific knowledge and expertise about the operations and business models of Bigtech firms and platform technology is incomplete. Moreover, the regulation of Bigtech finance involves something qualitatively different from what is done for traditional financial services, where the regulation is mostly sectoral (traditionally, banking, securities and insurance) and based on entities or activities, as elaborated below. These problems are compounded by information asymmetries that exist between Bigtechs on the one hand, and regulatory authorities on the other. Digital providers are notably reluctant to share basic information on their internal operations or methods of data storage due to commercial sensitivities and concern over unwanted scrutiny. These problems are magnified with respect to cybersecurity issues, where national authorities continue to largely rely on Bigtechs' cooperative spirit to monitor and assess systemic risks. Until recently most financial regulators lacked the power to compel or request information from Bigtechs, resulting in struggles to retrieve relevant information. Although EU regulators have now been granted the power to do so, they often struggle to interpret the data they receive from Bigtechs and lack the resources to deal with the pace of technological innovation. Thus, regulators often play catch up (James and Quaglia 2024).

Second, Bigtech finance is a notable example of a fragmented but interconnected regulatory regime because it touches upon, or rather cuts across, different policy areas that are traditionally 'siloed', that is to say, regulated separately and with different sectoral regulators responsible for oversight and enforcement within and without finance. Bigtech's business model and their vast gamut of financial and non-financial activities do not align with traditional regulatory perimeters and make them difficult to regulate and monitor. Since there is no lead regulator, responsibilities are divided across separate sectoral agencies (Boissay et al. 2021): not only multiple types of financial regulators – such as banking, securities, insurance and market infrastructure regulatory agencies – but also competition authorities, data regulators, cybersecurity experts (see Figure 1). All these regulators have distinct mandates, regulatory approaches and professional backgrounds.

To begin with, Bigtech finance involves several financial regulatory agencies, ranging from macro and micro prudential regulators (predominantly central banks and banking supervisors) to financial conduct authorities (e.g. securities markets regulators and anti-money laundering authorities). Prudential regulators are concerned about the financial stability implications of Bigtech finance. They tend to favour 'entity-based' regulation and the imposition of prudential rules (such as capital and liquidity requirements, or rules about internal governance) on licensed entities, which, therefore, require formal authorisation from regulators at the outset. Other entity-based prudential rules include the 'segregation' of the financial activities and nonfinancial activities of firms, and/or their designation as globally systemically-important if they exceed a certain threshold (Borio et al. 2022). Prudential authorities regularly monitor on-site and off-site the build-up of risks in the licensed entities, and can deploy several preventive instruments to prompt entities to modify excessive risk-taking behaviour.

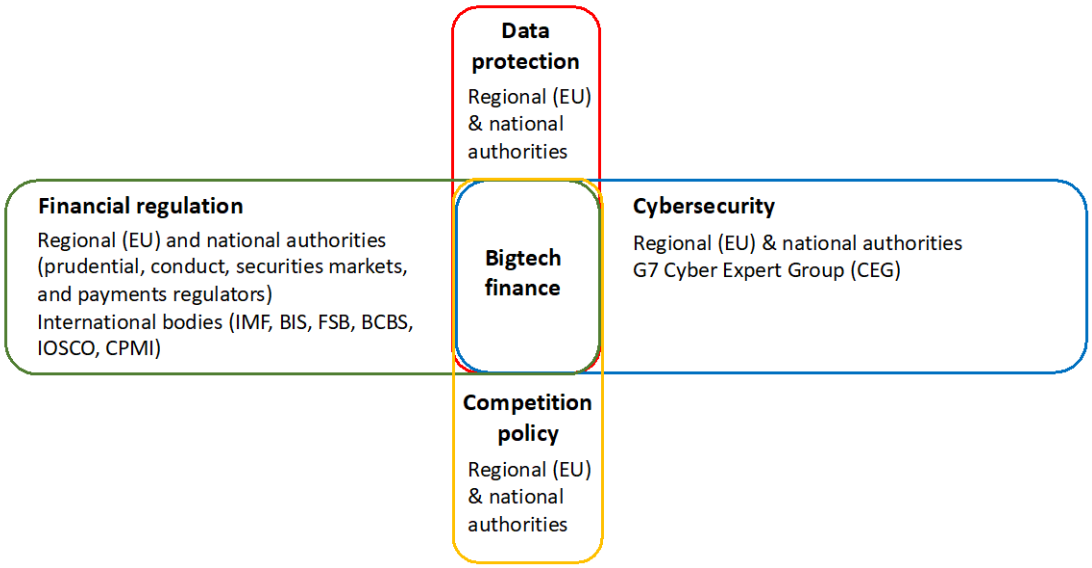
By contrast, securities regulators are primarily concerned with investor protection and market integrity. Regulation is applied to certain regulated activities, usually for market conduct purposes. Rules are generally prescriptive, and compliance is ensured by fines and other ex post enforcement measures. This approach must define activities very precisely, which is likely to provide opportunities for regulatory arbitrage because it is difficult to capture the fast evolution of Bigtech financial activities (Adrian 2021). Since the activity-based approach usually relies on ex-post enforcement, it is difficult to take ex-ante supervisory actions to modify risky behaviour. It is also not very effective for cross-border

activities, unless there is a global regulator or international agreements concerning cross-country enforcement actions (Adrian 2021).

The divisions among regulators are exacerbated by the involvement of a range of authorities outside finance, namely, competition authorities, data regulators and cybersecurity agencies, which have very different mandates, namely, to safeguard market contestability and anti-trust policy; safeguarding the rights of individuals to data privacy; the protection of networks and individual users from digital attacks usually aimed at accessing sensitive information or creating system-wide disruptions. These regulators also have different professional backgrounds: financial regulators are generally economists, competition and data protection authorities tend to recruit lawyers, and cybersecurity officials are commonly I.T. specialists. The different terminology, understandings and priorities attached to digital platforms that these diverse backgrounds generate serves as an additional challenge to facilitating inter-agency communication and coordination (James and Quaglia 2024).

Equally important, while there are well-established international standard-setting bodies in finance (such as the BIS, the IMF, the FSB, the BCBS etc) and financial regulatory agencies have a long history of cross-border cooperation that has, by and large, fostered a culture of trust between them, there are no equivalent international bodies for competition policy, data protection, and cyber security. To be sure, competition authorities have become accustomed to some degree of cross-border cooperation, whereas data regulators and cyber experts have less experience of working with their peers in other jurisdictions. Moreover, cooperation among these regulators at the international level is largely non-existent, and there are no international fora that bring them together on a systematic basis (James and Quaglia 2024). Even at the domestic level, inter-agency cooperation in this field is very limited (albeit in some jurisdictions, notably, the EU, some ad hoc fora have recently been established, as discussed in Section 5).

Figure 1: Bigtechs' fragmented but interconnected regulatory regime



Source: authors' own elaboration

The other major global challenge of Bigtech finance for the EU is that Bigtechs provide their services across borders, but they are subject to fragmented regulation and supervision, which remain national competences and vary considerably across jurisdictions. Thus, certain (few) jurisdictions (notably, China) have adopted entity-based regulation on Bigtechs, while other jurisdictions have adopted

activity-based regulation with varying degrees of stringency. Certain jurisdictions (i.e. the US and China) are home countries of Bigtechs, all the others are hosts. Home countries are more likely to adopt entity-based regulation because the Bigtechs are located within their jurisdictional borders. However, to date, the main home jurisdictions for Bigtechs have adopted an inconsistent approach, with China adopting entity-based regulation, while the US has not. It is difficult for host countries to adopt entity-based regulation because Bigtechs headquarters are located outside their jurisdictional borders. Consequently, hosts tend to adopt activity-based regulation (Bains et al. 2022), although with different degrees of stringency. Furthermore, jurisdictions have different types and stringency of regulation concerning other policies – such as market competition, data privacy, cybersecurity - interlinked with Bigtech finance.

The near absence of international standards for Bigtech finance means that there is no regulatory harmonisation across borders, but also that jurisdictions do not have a minimum level of regulation they should comply with (unlike, for instance, minimum capital requirements for banks). Jurisdictions have different incentives to set (or not) international standards, depending on whether they are home or host. Thus, home jurisdictions are generally reluctant to set international standards, as they think that they can deal with the risks posed by Bigtech finance via domestic regulation. They also have different incentives to tighten up (or not) domestic rules on this matter, depending on their exposure to negative cross-border externalities related to Bigtech finance and their vulnerability to regulatory failures in this area. By contrast, host jurisdictions, in particular large ones, such as the EU, which tend to have more regulatory clout in international fora, have an incentive to promote international standards on Bigtech finance to reduce the risk of 'imported' financial risks generated by Bigtechs that are not sufficiently well regulated in their home countries. In the absence of international soft law on the matter, host jurisdictions concerned about some of the negative implications of Bigtech finance for financial stability, market competition, data privacy, cyber security etc have an incentive to strengthen their domestic activity-based regulation and to expand its extraterritorial reach.

A final point is worth considering in this respect. In certain financial sectors, notably, banking, the EU has mostly downloaded international standards (such as the Basel accords) into EU legislation because the BCBS is a well-established body that has set bank capital requirements since the late 1980s (Quaglia 2014). There is no comparable international standard setter for Bigtech finance. This could create room for manoeuvre for the EU to be a rule-maker, rather than a rule-taker. It is true that the main Bigtechs are headquartered outside the EU. Yet, the EU could leverage its influence as a large and lucrative market for foreign Bigtechs looking to expand their financial services provision and/or to circumvent domestic restrictions at home. In addition, Chinese bigtechs currently have a limited footprint in the EU and Chinese authorities have demonstrated little interest is in shaping international standards to date. This provides greater scope for the EU to forge a closer regulatory partnership with US authorities to shape global developments. US-EU cooperation around data protection, and, more recently, cyber security (through the G7 CEG), provides a precedent for how the EU can exploit its leverage as a single market to shape new global rules, even as a host regulator.

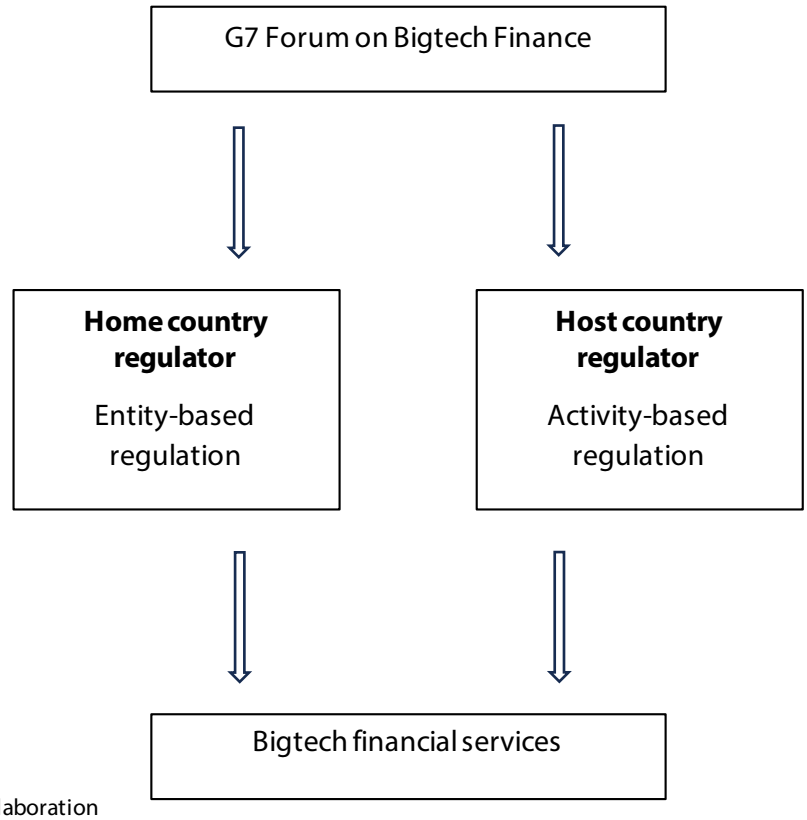
5. POLICY RECOMMENDATIONS

In light of the far-reaching implications of Bigtech finance for the EU's growth model (Section 2), the development of the EU's regulatory framework in this field (Section 3), as well as the global challenges that the EU has to confront (Section 4), we propose the following recommendations. These begin with recommendations concerning the regulation of Bigtechs in finance internationally (recommendations 1 and 2), and the role of the EU in fostering cross-border cooperation in this field (recommendation 3), before focusing on the intra-EU regulation of Bigtech finance (recommendation 4) and the facilitating role of the European Parliament (recommendation 5).

Recommendation 1

The first recommendation is to consider the **adoption of a 'holistic' or 'hybrid' approach at the international level, complementing activity-based regulation in host countries with entity-based regulation in home countries** (e.g. Bains et al. 2022; Ehrentraud et al. 2022). Host supervisors should actively use all their existing powers — such as indirect supervision through regulated entities (notably, banks) and activity-based regulations (Carstens 2023), in so doing improving the resilience of entities themselves (Borio et al. 2022). Moreover, digital platforms undertake a variety of financial and non-financial activities, and therefore many of their risks originate from outside the financial sector (Ehrentraud et al. 2022). That also means that the principal regulator of the entity might not be a financial regulator. Whatever the regulatory agency is, it should work closely with financial regulators as well as regulators that oversee competition, data privacy, cyber security, and consumer protection.

Figure 2: Hybrid approach to strengthening the international oversight of Bigtech finance



Source: authors' own elaboration

Within the domain of an entity-based approach, there are several alternatives (see Carstens 2023). 1) The 'restriction' approach would prohibit Big Techs from engaging in regulated financial activities altogether, although such a move would elicit strong opposition from Bigtechs and their loyal customer base. 2) The 'segregation' approach would require Bigtechs to group their financial activities under a financial holding company, subject to prudential requirements and ring-fenced (i.e. segregating a part of a company's financial assets from the rest). This approach could weaken the business case for Bigtechs to offer financial services. 3) The third approach would involve the creation of a new regulatory category for Bigtechs with significant financial activities, a Bigtech financial group, subject to requirements at the group-wide level. This approach covers both the parent and its financial and non-financial entities, with a view to monitoring the risks of interdependencies between them. Since Bigtechs operate in a variety of jurisdictions, in some cases, it may be difficult to identify the home supervisor and smooth cooperation between home and host authorities requires a considerable degree of trust. It is also tricky for investors and consumers to identify which authority is responsible for handling complaints (ESA 2023).

Recommendation 2

The second recommendation is to **improve international cooperation between different sectoral regulators by establishing a high level multi-sectoral regulatory body or forum** bringing together financial regulators, competition authorities, data regulators and cyber-experts. In the first instance, this forum could be organised around the G7 countries, and would thus build on the precedent established by the G7 Cyber Expert Group. In this respect, the BIS, the IMF and the FSB could set up or act as sandboxes. It might be more feasible for these bodies to take the lead because in finance, unlike for competition, data protection and cybersecurity, there is quite a well-established tradition of cross border cooperation and gathering of domestic regulators in international bodies. Some of these bodies are also relatively well-resourced. The EU should actively support the establishment of such an international forum and EU-level bodies as well as national competent authorities of the G7 member states should participate in it.

In the absence of the establishment of a designated G7 body or forum for bigtech firms, **the EU could promote the creation of an International Digital Finance Network** - modelled on the International Competition Network - composed of national and EU competent authorities with responsibilities covering different aspects of digital finance, including financial stability, investor protection, competition, data protection and cybersecurity. Although this would be a looser arrangement, a designated network could nevertheless serve a valuable role in strengthening dialogue, information sharing and promotion of best practices among participants from the G7 countries, with a view to expanding its membership and/or establishing a more formal institutional basis for cooperation in the future.

Recommendation 3

The third recommendation is to foster **stronger bilateral cooperation over bigtech finance between the EU and US and between the EU and UK**, as a precursor to international cooperation in multilateral fora. The EU and US could lead in the establishment of the G7 Forum and/or the International Digital Finance Network, as outlined above. The discussion of closer cooperation on Bigtech finance regulation is also an area of close alignment with the UK, and could become a standing item for discussion on the newly-established biannual EU-UK Financial Regulatory Forum.

Failing this, **the EU could adopt a unilateralist approach**, acting as pace-setter internationally by exploiting first mover advantages. This would involve issuing new EU rules in this domain first and then seeking to upload those rules to international fora, or cross-load them to third jurisdictions. This could be done through the so-called 'Brussels effect' (Bradford 2021) for the Bigtechs that provide their financial services across the Single Market and also by issuing EU rules with extraterritorial reach (or the likes). The EU has already taken steps in these directions by adopting the DSA, the DMA, the DORA and the MICA (Centre for European Reform 2021) and could continue along this path.

Recommendation 4

The fourth recommendation is to **improve cooperation between different sectoral regulators in the EU** by establishing a multi-sectoral regulatory forum in the EU. This could be based on expanding and developing the role of the new High-Level Group established by the DMA – for example, by ensuring a more prominent role for central banks, prudential regulators and securities markets regulators. At present, the High-Level group brings together representatives from the European Data Protection Supervisor and European Data Protection Board, the European Competition Network, the Consumer Protection Cooperation Network, the Body of the European Regulators for Electronic Communications, and the European Regulatory Group of Audiovisual Media Regulators.[16] Initially, the scope of the EU level cross-sectoral body would be limited to knowledge development, information sharing, capacity building as well as joint interactions with stakeholders (see ESA 2023). Following the same logic, EU member states should also set up parallel cross-sectoral fora at the domestic level.

Recommendation 5

The **final recommendation concerns the facilitating role of the European Parliament**. MEPs should seek to leverage affinities and the expertise of national legislators, from both inside and outside the EU, in the regulation and supervision of Bigtech platforms. The EP could take the lead in establishing working groups to monitor and study Bigtechs, and monitor future developments, with a view to increasing awareness and transparency in this area, and to support the strengthening of knowledge and expertise of legislators in this highly technical field. In addition to working groups of EP and national legislators, a Bigtech working group could also be established with members of the US Congress and UK Parliament that are supportive of more stringent Bigtech regulation.

[16] https://digital-strategy.ec.europa.eu/en/news/digital-markets-act-commission-creates-high-level-group-provide-advice-and-expertise-implementation

REFERENCES

- Adrian, T. (2021) 'BigTech in Financial Services - speech', International Monetary Fund, Washington, 16 June, available at https://www.imf.org/en/News/Articles/2021/06/16/sp061721-bigtech-in-financial-services
- Alter, K.J. and Raustiala, K. (2018) 'The rise of international regime complexity', *Annual Review of Law and social Sciences* 14: 329-349.
- Bains, P. et al. (2022) *BigTech in Financial Services: Regulatory Approaches and Architecture*, International Monetary Fund, Washington.
- Bains, P., Arif, I., Melo, F. and Sugimoto, N. (2022) *Regulating the Crypto Ecosystem: The Case of Stablecoins and Arrangements* IMF, International Monetary Fund, Washington.
- Banque de France (2022) 'Focus: the G7 Cyber Expert Group', available at https://www.banque-france.fr/en/economics/international-relations/international-groups-g20g7/focus-g7-cyber-expert-group
- Bassens, D. and Hendrikse, R. (2022) 'Asserting Europe's technological sovereignty amid American platform finance: Countering financial sector dependence on Big Tech?', *Political Geography* 97: 1026-48.
- Bank for International Settlements (2019) 'Big tech in finance: opportunities and risks', *Annual Economic Report*, Basel.
- Bernards, N. and Campbell-Verduyn, M. (2019) 'Understanding technological change in global finance through infrastructures', *Review of International Political Economy* 26 (5): 773-89.
- Boissay, F., Ehlers, T., Gambacorta, L. and Shin, H-S. (2021) *Big techs in finance: on the new nexus between data privacy and competition*, Bank for International Settlements Working Paper N. 970, Basel.
- Borio, C., Claessens S., and Tarashev, N. (2022) *Entity-based vs activity-based regulation: a framework and applications to traditional financial firms and big techs*, Financial Stability Institute Occasional Paper N. 19, Basel.
- Bradford, A. (2020) *The Brussels Effect: How the European Union Rules the World*, New York, Oxford University Press.
- Broeders, D., Cristiano, F., Kaminska, M. (2023) 'In search of digital sovereignty and strategic autonomy: Normative power Europe to the test of its geopolitical ambitions', *Journal of Common Market Studies* 61 (5): 1261-1280.
- Campbell-Verduyn, M. and Lenglet, M. (2022) 'Imaginary failure: RegTech in finance', *New Political Economy* 28 (3): 468-482.
- Campbell-Verduyn, M., Goguen, M., & Porter, T. (2017) 'Big data and algorithmic governance: The case of financial practices', *New Political Economy* 22 (2): 219–236.
- Carstens, A. et al. (2021) *Regulating big techs in finance*, Bank for International Settlements Bulletin No 45, Basel.
- Carstens, A. (2019) 'Data, technology and policy coordination – Speech', Bank for International Settlements, Basel, 14 November.
- Carstens, A. (2023) 'Big techs in finance: forging a new regulatory path - Speech', Bank for International Settlements, Basel, 8 February.
- Centre for European Reform (2021) *Can the EU set a global rulebook for big tech?,* London, June.
- Clarke, C. (2019) 'Platform lending and the politics of financial infrastructures', *Review of International Political Economy* 26 (5): 863–85.
- Crisanto, J. et al. (2021) *Big tech regulation: what is going on?,* Financial Stability Institute Insights, Basel.

- Crisanto, J. et al. (2022) *Big tech interdependencies – a key policy blind spot*, Financial Stability Institute, Basel, July.
- Doerr, S., Frost, J., Gambacorta, L., Shreeti, V. (2023) *Bigtechs in finance*, Bank for International Settlements Working Paper N. 1129, Basel.
- Ehrentraud, J., Lloyd Evans, J., Monteil, E. and Restoy, F. (2022) *Big tech regulation: in search of a new framework*, Financial Stability Institute Occasional Paper N. 20, Basel.
- Euractive (2022) 'Scant resources might threaten enforcement on Big Tech, EU data protection bodies warn', 13 September.
- European Commission (2023) *Digital Euro Package*, Brussels, June.
- European Central Bank (2023) 'Eurosystem proceeds to next phase of digital euro project', Frankfurt, 18 October, available at https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr231018~111a014ae7.en.html
- European Parliament (2021) 'Stablecoins Private-sector quest for cryptostability', Briefing, Brussels, November.
- Euro Summit Statement (2021), 25 March, Brussels.
- European Supervisory Authorities (ESA) (2023) *Joint Report on Digital Finance*, https://www.eiopa.europa.eu/publications/joint-esas-report-digital-finance_en
- European Union Agency for Cyber Security (ENISA) (2021) 'EU Cybersecurity Initiatives in the Finance', available at https://www.enisa.europa.eu/publications/EU_Cybersecurity_Initiatives_in_the_Finance_Sector
- Farrell, H. and Newman, A. (2019) *Privacy and Power: The Transatlantic Struggle over Freedom and Security*, Princeton: Princeton University Press.
- Federal Reserve (2021) *Preconditions for a general-purpose central bank digital currency*, FED Notes, Washington, February.
- Financial Stability Board (FSB) (2018) *Cyber Lexicon*, Basel, November.
- Financial Stability Board (FSB) (2019a) *BigTech in Finance: Market developments and potential financial stability implications*, Basel, December.
- Financial Stability Board (FSB) (2019b) *Third-party dependencies in cloud services: Considerations on financial stability implications*, Basel, December.
- Financial Stability Board (FSB) (2020) *Effective Practices for Cyber Incident Response and Recovery*, Basel, October.
- Financial Stability Board (FSB) (2023a) *Global Regulatory Framework for Crypto-Asset Activities*, Basel, July.
- Financial Stability Board (FSB) (2023b) *High-level Recommendations for the Regulation and Supervision of global stablecoin arrangements*, Basel, July.
- Foroohar, R. (2012) *The Guardian*, 8 November.
- Gambacorta, L., Khalil, F. and Parigi, B. (2022) *Big Techs vs Banks*, Bank for International Settlements Working Paper N. 1037, Basel, August.
- Hendrikse, R., Meeteren, M. van, and Bassens, D. (2019) 'Strategic coupling between finance, technology and the state: cultivating a Fintech ecosystem for incumbent finance', *Environment and Planning A: Economy and Space* 52: 1516–1538.
- House of Lords (2021) *Central Bank Digital Currencies: a Solution in Search of a Problem?* London, January.
- Klinge, TJ., Hendrikse, R., Fernandez, R., Adriaans, I. (2022) 'Augmenting digital monopolies: a corporate financialization perspective on the rise of Big Tech', *Competition & Change* 27 (2): 332-353.

- James, S. and Quaglia, L. (2022) 'Epistemic contestation and interagency conflict: The challenge of regulating investment funds', *Regulation & Governance* 17 (2): 346-362.
- James, S. and Quaglia, L. (2023) 'Why are international standards not set? Explaining "weak" cases in shadow banking regulation', *Journal of Public Policy*, doi:10.1017/S0143814X23000417
- James, S. and Quaglia, L. (2024) 'Emergent Regime Complexity and Epistemic Barriers in 'Bigtech' Finance', *New Political Economy*
- James, S. and Quaglia, L. (2024), 'Banks, bigtechs and the noisy politics of geostrategic linkage in Europe', paper presented at the workshop 'Power struggles and transformative forces: The transformations of the banking sector' held at the University of St Gallen, 26-27 October.
- Joint European Supervisory Authority (2022) Response to the European Commission's Call for Advice on digital finance and related issues, 31 January.
- Langley, P. and Leyshon, A. (2017) 'Platform capitalism : the intermediation and capitalization of digital economic circulation', *Finance and Society* 3 (1): 11-31.
- Langley, P. and Leyshon, A. (2021) 'The platform political economy of FinTech: reintermediation, consolidation and capitalisation', *New Political Economy* 26: 376–388.
- Panetta, F. (2021) 'Stay safe at the intersection: the confluence of big techs and global stablecoins - Speech', European Central Bank, Frankfurt, 8 October.
- Panetta, F. (2022a) 'The digital euro and the evolution of the financial system - Speech', European Central Bank, Frankfurt, 15 June.
- Panetta, F. (2022b) 'For a few cryptos more: the Wild West of crypto finance - Speech', 25 April.
- Panetta, F. (2023) 'The cost of not issuing a digital euro - Speech', European Central Bank, Frankfurt, 23 November.
- Petit, N. (2020) *Big Tech and the Digital Economy: The Moligopoly Scenario*, Oxford: Oxford University Press.
- Petralia K., Philippon, T., Rice, T., and Véron, N. (2019) 'Banking Disrupted? Financial Intermediation in an Era of Transformational Technology, Geneva Report, CEPR, September.
- Quaglia, L. (2022) *The Perils of International Regime Complexity in Shadow Banking*, Oxford: Oxford University Press.
- Quaglia, L. (2014) The European Union and Global Financial Regulation, Oxford University Press, Oxford.
- Rolf, S. and Schindler, S. (2023) 'The US–China rivalry and the emergence of state platform capitalism', *Environment and Planning A: Economy and Space* 55 (5): 1255-1280.
- Stulz, R.M. (2019) 'FinTech, BigTech, and the Future of Banks', *Journal of Applied Corporate Finance* 31(4):86-97
- van Dijck, J. Poell, T. and De Waal, M. (2018) *The Platform Society: Public Values in a Connective World*, Oxford: Oxford University Press.
- Villeroy de Galhau, F. (2023) 'Big techs in finance: a bildungsroman that is far from over – Speech', Banque of France, Paris, 9 February.
- Waller, C. (2021) 'CBDC - A Solution in Search of a Problem? – Speech', Bank for International Settlements, Basel, 5 August.
- Withers, I. and Jones (2021) 'For bank regulators, tech giants are now too big to fail', *Reuters*, 20 August

'Bigtech finance' — i.e. the provision of financial services by large digital conglomerates - has considerable implications for the EU's growth model and raises multiple regulatory concerns about financial stability; competition and market concentration; data protection; cybersecurity and operational resilience. Bigtechs also have potential geostrategic implications because the largest digital platforms are headquartered outside the EU. To address these global challenges, this study makes

This document was provided by the Economic Governance and EMU Scrutiny Unit at the request of the ECON Committee.

PE 755.724
IP/A/ECON-ED/IC/2023-089

Print ISBN 978-92-848-1539-5 | doi:10.2861/913891 | QA-02-24-057-EN-C
PDF ISBN 978-92-848-1540-1 | doi:10.2861/78436 | QA-02-24-057-EN-N