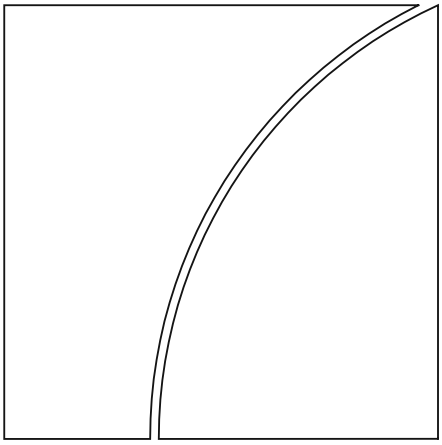
Financial Stability Institute

# FSI Insights

on policy implementation

No 44



# Big tech interdependencies – a key policy blind spot

By Juan Carlos Crisanto, Johannes Ehrentraud, Marcos Fabian and Amélie Monteil

July 2022

JEL classification: G18, G21, G23, G28, L41, L51

Keywords: big techs, business model, interdependencies, activity-based regulation, entity-based regulation, operational resilience, financial stability

BANK FOR INTERNATIONAL SETTLEMENTS

FSI Insights are written by members of the Financial Stability Institute (FSI) of the Bank for International Settlements (BIS), often in collaboration with staff from supervisory agencies and central banks. The papers aim to contribute to international discussions on a range of contemporary regulatory and supervisory policy issues and implementation challenges faced by financial sector authorities. The views expressed in them are solely those of the authors and do not necessarily reflect those of the BIS or the Basel-based committees.

Authorised by the Chair of the FSI, Fernando Restoy.

This publication is available on the BIS website (www.bis.org). To contact the BIS Media and Public Relations team, please email press@bis.org. You can sign up for email alerts at www.bis.org/emailalerts.htm.



ISSN 2522-249X (online)
ISBN 978-92-9259-583-8 (online)

# Contents

# Big tech interdependencies – a key policy blind spot[1]

## Executive summary

**The increasingly prominent role of large technology firms (big techs) in the financial sector has raised questions about their inner workings and regulation.** Big techs have already gained a substantial footprint in parts of financial services; and the trend towards more digitalisation, which the Covid-19 pandemic has accelerated, has allowed them to fortify their market positions even further. While big tech business models vary across markets and jurisdictions, they also share characteristics that could represent a major source of disruption to the financial system and give rise to a range of policy concerns. One attribute of big techs' business model that has so far received less attention, and is therefore less well understood, are the implications of their internal and external interdependencies on the financial system.

**Big tech activities underpin closely connected digital platform ecosystems.** Such an ecosystem, which has a digital platform at its centre, is run by financial and non-financial entities that form part of a big tech group. Other participants in the ecosystem are third-party entities that offer products and services on the platform as well as individuals and businesses that use them. By using cutting-edge technology, big tech entities take advantage of users' personal data as an input to create further user activity and generate more data. This ability to enable active interaction among different participants in their ecosystem is a key element underpinning the business models of big techs. It may not be surprising therefore that significant intragroup dependencies and external interconnections are integral parts of the big tech business model.

**The objective of this paper is to explore the interdependencies inherent in big tech's business models.** This assessment is based on the business models of six big techs around the world (Alibaba, Amazon, Grab, Jumia, Mercado Libre and Rakuten). Due to the lack of a comprehensive source of information on their organisational structure, activities and the risks involved, this paper has pieced together a view of their business models using a variety of publicly available information such as securities prospectuses, annual reports, expert press reports and other investor resources.

**The analysis of individual big tech business models points to several common features**. Their core activity is usually complemented by a wide array of services, particularly financial and technology ones. Another common feature relates to the integration of different big tech activities into the same platform using "ecosystem binders". These are applications and tools that facilitate and promote the use of the entire ecosystem such as super apps and loyalty schemes. Big techs also commonly show a drive to grow and expand to new markets. Finally, big tech business models rely on a strongly connected digital platform ecosystem that generates strong intragroup and external interdependencies.

**Big techs' drive to grow is reflected in different stages of their development, generating both regional and global big techs.** The more services a big tech platform offers, the more attractive it could be for its users. The continuous expansion of big techs into new markets can be observed through various indicators related to their operations such as number of jurisdictions and clients, level of revenues and business areas. These indicators show that Alibaba and Amazon operate globally in a wide number of business areas and have a large customer base. Other big techs such as Grab, Jumia, Mercado Libre and Rakuten have a regional focus, serve a relatively smaller customer base and operate in a limited number of business segments. They are, however, expanding towards new markets.

[1] By Juan Carlos Crisanto (Juan-Carlos.Crisanto@bis.org) Johannes Ehrentraud (johannes.Ehrentraud@bis.org) and Amélie Monteil (Amelie.Monteil@bis.org), Bank for International Settlements, and Marcos Fabián (fabian@asbasupervision.org), Association of Supervisors of Banks of the Americas. The authors are grateful to Patrick Armstrong, Jamie Lloyd Evans, Jon Frost, Jermy Prenio and staff from the Office of the Superintendent of Financial Institutions (OSFI) Canada for helpful comments and to Theodora Mapfumo for administrative support.

**Intragroup dependencies help big techs achieve economies of scale but raise risks.** Financial and non-financial entities that form part of the big tech group use common payment systems to facilitate transactions across the entire ecosystem. In addition, they use the same technological infrastructures, computer applications and analytical tools to process information relevant for the group. They also rely on a common credit scoring system to evaluate clients and share their data to make the ecosystem work. These intragroup dependencies raise the potential for difficulties regarding one or more parts of big tech activities to spill over across the entire group, which may have a negative impact on their provision of regulated financial services.

**The activities of big techs and financial institutions are increasingly intertwined and have the potential to give rise to meaningful external interdependencies.** Both offer financial products and services through a variety of partnerships, including: (i) strategic alliances to facilitate payments in the big tech ecosystem; (ii) white labelling arrangements through which big techs perform customer interface functions; (iii) banking-as-a-service partnerships that allow big techs to integrate financial products from different providers into their platform; (iv) pre-screening services by big techs to identify whether customers are eligible for certain financial products; and (v) arrangements to originate and/or distribute lending and insurance products. The lack of transparency around these arrangements makes it complex to assess the type and level of risks to which financial institutions are exposed.

**Financial institutions and regional big techs rely heavily on technology services provided by global big techs, and this is likely to deepen going forward.** Most financial institutions already use some form of public cloud and related data analytical services. The provision of these services is highly concentrated, with only a few big tech companies dominating the market. As a result of their investment in cutting-edge technology, this dependence is likely to increase going forward. This will exacerbate operational and concentration risks as well as the systemic vulnerabilities that may arise if big techs experience significant disruptions. These disruptions may be amplified by regional big techs and could have a broader impact on the global economy.

**The existing regulatory framework was not formulated with closely connected digital platform ecosystems in mind and may miss the risks arising from interdependencies.** Big techs are subject to the regulatory regimes that govern the financial sectors they are active in (eg banking, payment and insurance) which do not differentiate between big techs and other companies active in the same financial sector. Yet regulatory instruments currently available under sectoral frameworks were not designed to mitigate the risks created by interdependencies inherent in big tech business models. It is therefore not surprising that sectoral laws and regulations have certain blind spots when applied to big tech groups.

**Addressing risks arising from interdependencies may require the development of specific entity-based rules for big tech operations in the financial sector.** These rules could take the form of a new regulatory framework that allows authorities to control risks emerging from the combination of financial and non-financial activities. This framework would benefit from imposing requirements at the group level, including on strengthening operational resilience.

**In the short term, authorities can rely on an indirect approach to mitigate the financial stability risks.** There are a number of options available to them. One is to identify risks stemming from interdependencies for regulated financial entities that are members of big tech groups and evaluate potential risk mitigants. Another is to assess these entities' abilities, and those of other regulated financial entities that partner with big techs or depend on their services, to withstand and mitigate disruptive events, including cyber attacks, and take measures to further strengthen operational resilience if needed. Yet another option for authorities is to intensify their monitoring efforts in relation to critical third-party service providers and, depending on the regulatory framework, use direct oversight powers over them. In this context, authorities could benefit from sharing information on their regulatory approaches and supervisory practices with each other.

# Section 1 – Introduction

1. **Digital services provided by large digital platform companies have become ubiquitous across the globe.** These companies, big techs, now serve a myriad of customers who regularly order products online, send messages via apps on mobile phones or check their email or social media accounts.[2] By expanding their services, big techs have grown large, and several of them now have market capitalisations that exceed those of the largest financial institutions.[3]

2. **Big techs have already gained a substantial footprint in parts of financial services.** In some segments and regions, they have emerged as key players over the past decade.[4] Big techs offer a particularly broad range of financial services in emerging market and developing economies. In some of these markets, they have come to reach dominant positions in payments, credit and other services. Big techs dominate, for example, the mobile payments markets in China and India (Feyen et al (2021)). During the pandemic, big techs saw strong growth, including in financial services such as payments and credit, which appears to have helped them to fortify their market positions even further (FSB (2022)). Going forward, big techs may also decide one day to leverage their immense user base for offering stablecoins.[5]

3. **Big techs operate highly interconnected platform ecosystems.** Their platform-based business models, which are built on the use of large amounts of personal data, rest on enabling direct interactions among a large number of users. Behind the scenes, big tech platforms are powered by multiple legal entities that big techs have within their groups. These financial and non-financial entities share data and provide services to each other to make the digital platform ecosystem work, ie they are dependent on each other.

4. **Strong external interconnections are an integral part of big techs' business model.** Big techs not only engage in partnerships with financial institutions to offer financial services but also provide them with technology services such as cloud computing and data analytics. These services have become critical to the operation of incumbent financial institutions, creating a situation of dependency with big techs.[6] Some big techs are also customers and not providers of cloud computing services, creating a network of third-party interdependencies. Taken together, this supply and demand for technology services by big techs creates external interdependencies among big techs and with financial institutions.

5. **Internal and external interdependencies come with specific risks, in particular to operational resilience.** A failure in one part of the big tech group could render others unable to function; or disrupt the flow of data between big tech entities. Similarly, operational incidents at third-party service providers, including other big techs, could result in outages or data breaches, with potential knock-on effects on the platform ecosystem and its users.[7] Given the active participation of big techs in the financial services industry, these risks are particularly relevant for financial regulators whose main objective is to keep the financial system safe and sound, and well functioning from an operational point of view.

6. **These risks are hard to assess due to the dearth of information on internal and external dependencies.** Big techs that are publicly traded companies are typically required to disclose information

[2] The BIS and Financial Stability Board (FSB) define big techs as large companies whose primary activity is digital services. See BIS (2019), Carstens et al (2021) and FSB (2019a).

[3] See Carstens (2018), Chui (2021) and Feyen et al (2021).

[4] See Frost et al (2019) and Croxson et al (2022).

[5] A project initiated by Facebook/Meta to issue stablecoins, called Diem, was abandoned in early 2022. See www.diem.com/en-us/.

[6] See, eg, FSB (2019b).

[7] For example, the outage of third-party cloud services could leave financial entities within a big tech group unable to access their data or run their applications when they need to.

about their financial performance (eg the Securities and Exchange Commission's annual public 10-K reports). They may not be required, however, to disclose comprehensive information on their diverse business activities, leaving investors, competitors and regulators less aware of how exactly they create and extract value from their ecosystems.[8] Without this information, it is especially challenging to understand the corporate structures underpinning the collaboration between big techs and financial institutions, particularly outside their primary domicile (FSB (2022)). Overall, while the platforms of the ecosystems are visible, the machinery that makes them work is largely removed from view, complicating any efforts by outside parties to fully understand their entire ecosystem exposure.

7. **The purpose of this paper is to assess the interdependencies inherent in big tech's business models and offer some policy considerations for financial authorities**. The assessment of interdependencies is based on the business models of six big techs: Alibaba, Amazon, Grab, Jumia, Mercado Libre and Rakuten (Table 1).[9] Due to the lack of a comprehensive source of information on their organisational structure, activities and risks involved, this paper has pieced together a view of their business models using a variety of publicly available information such as securities prospectuses, annual reports, expert press reports and other investor resources. Section 2 describes big tech business models. Sections 3 and 4 review intragroup and external interdependencies inherent in big techs' business models. Section 5 outlines the regulatory implications of how big techs provide financial services and the tools financial authorities have at their disposal to address risks related to intragroup and external dependencies. Section 6 offers some concluding remarks.

[8] See Strauss et al (2021).

[9] Aside from the big techs considered in this paper, there are others (eg Apple, Facebook/Meta, Google/Alphabet, Microsoft) whose role in the financial sector and potential impact on non-financial risks and financial stability could be analysed in future research.

## Big techs – selected indicators

Table 1

| | Alibaba/ Ant Group | Amazon | Grab | Jumia | Mercado Libre | Rakuten |
|---|---|---|---|---|---|---|
| Began operations | 1999 | 1994 | 2012 | 2012 | 1999 | 1997 |
| Headquarters | Hangzhou, CN | Seattle, US | Singapore, SG | Berlin, DE | Buenos Aires, AR | Setagaya-ku, JP |
| Market capitalisation (USD) and credit rating* | 260 bn (A+) | 1,400 bn (AA) | 21 bn (B–) | 0.8 bn (na) | 53 bn (BB+) | 13 bn (BB+) |
| Key products and services | E-commerce[#] Technology & financial services. | Online marketplace for books[#] Wide range of goods. Technology & financial services. | Mobility services[#] Food delivery. Digital payments. | E-commerce[#] Logistics. Payment services. | E-commerce[#] Logistics. Financial services. | E-commerce[#] Financial services. Tele-communication. |
| Markets with commercial presence | China[#] Global, particularly in the United States and Europe, with deliveries in over 190 countries. | United States[#] Global, with 13 country-specific websites and deliveries in over 100 countries. | Singapore[#] Operates in 8 countries in Southeast Asia. | Nigeria[#] Operates in 11 countries in Africa. | Argentina[#] Operates in 17 countries in South America and in the United States. | Japan[#] Global in over 30 countries, particularly in the United States, Europe and Asia. |
| Number of users[@] | 1,280 m active consumers | 200 m Prime members | 27.7 m monthly transacting users | 8 m annual active consumers | 139.5 m unique active users | 127 m active Rakuten IDs |
| Revenue[&] | 109.5 bn revenue at 31/03/2021 | 469.8 bn net sales at 31/12/2021 | 0.7 bn revenue at 31/12/2021 | 0.2 bn revenue at 31/12/2021 | 7.1 bn net revenue at 31/12/2021 | 13.7 bn revenue at 31/12/2021 |

* S&P LT credit ratings. First column shows data for Alibaba.

[#] Refers to products and services originally provided by the company or markets where it started to operate.

[@] The definition of the number of clients differs among the companies. All cited numbers come from the annual reports of the companies.

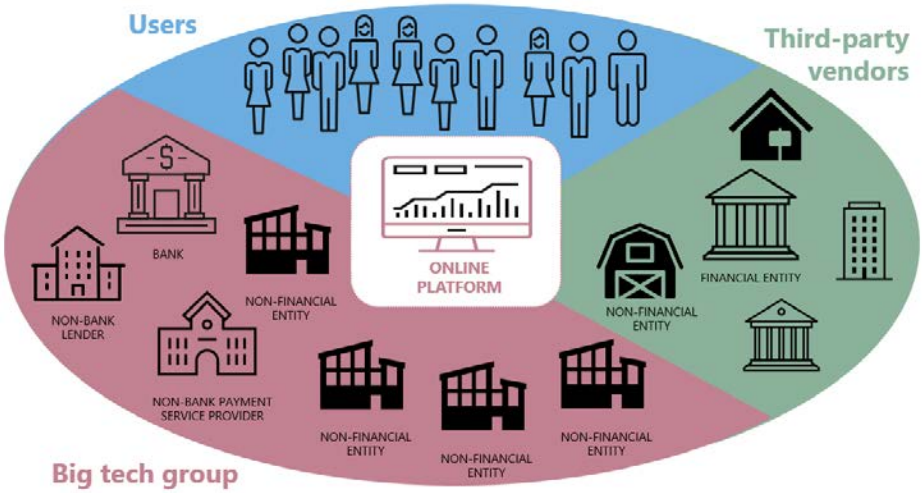
[&] The definition of revenues (in USD, rounded to one decimal) differs among the companies. All cited numbers come from the annual reports of the companies.

Sources: Public sources; FSI.

## Section 2 – Big tech business models

8. **The core of a big tech's business model is a multi-sided online platform which sits at the heart of its digital ecosystem**. This platform, which is operated by financial and non-financial entities that are members of a big tech group and use common IT systems and data, enables direct interactions between different types of participants (Graph 1). Individuals and businesses, as users of the platform, may buy or obtain products and services or conclude contracts on the platform. This may be done with a big tech entity as counterpart, or a third-party vendor which uses the platform to provide its services either in competition with big tech entities (eg independent merchants on an e-commerce platform) or in partnership with them (eg Apple and Goldman Sachs credit card partnership).

Big tech ecosystem — Graph 1




Source: Authors' conceptualisation.

9. **Although big tech business models vary across markets, they share several common features.** Several big techs have a privileged position in the retail e-commerce market; others are better known as successful developers of technological devices; and some are key providers of technology services (eg cloud and artificial intelligence solutions). Moreover, while some are focused on a particular region, others have significant global operations. Despite these differences, big tech business models share the following common features: their offering typically includes core, financial and technology services; their activities rely on ecosystem binders;[10] the incentive to continuously widen and deepen their activities; and the internal and external interdependencies in their operations.

### Core, financial and technology services

10. **Big techs generally offer three types of service: core services, financial services and technology services.** On the one hand, big techs' core activities allow them to collect data on a large network of users.[11] This information is critical to personalise their core activities and further develop the range of products and services offered. On the other hand, financial services usefully complement and reinforce their core activities, and allow big techs to collect additional and different types of data on their

[10] Applications and tools that integrate the entire ecosystem and facilitate and promote its use.

[11] Core services, which we define as activities at the core of a big tech's initial business plan, typically generate the lion's share of its revenues. "Core" does not denote "most important" as big techs may focus on other activities due to growth patterns or other strategic considerations.

users from their different business lines. Lastly, although big techs tend to offer a wide array of additional services, some of them have become significant IT services providers for both financial and non-financial institutions. As indicated in Table 2, the services offered by the big techs under analysis include:

- **Core services.** While e-commerce is the main business of Alibaba, Amazon, Mercado Libre, Jumia and Rakuten, Grab is a leading mobility – in particular ride hailing – platform. Despite this convergence, there are relevant examples of big techs outside our sample whose principal activity is not e-commerce. For instance, for Facebook/Meta it is social media, for Google/Alphabet online search and for Microsoft technology.
- **Financial services.** JumiaPay provides payment services to facilitate e-commerce transactions on the Jumia platform and generates data that can be used for marketing and credit scoring. Grab uses the data collected on its drivers and merchants, through both mobility and financial services, to offer loans to its ecosystem members.[12] The Alipay mobile app provides customers with one-stop shop digital payment and financial services. Amazon Pay offers customers a well integrated checkout option, using their Amazon account, to pay both on Amazon and on partner websites.
- **Technology services.** Rakuten developed its own artificial intelligence tool, AIris, which leverages on purchasers' data to perform intelligent target prospecting. Alibaba and Amazon are prominent providers of cloud computing services and associated data analytics, artificial intelligence and machine learning analytical tools. In fact, Amazon is reported to hold a 32% share of the cloud provider market.[13]

Service offerings by big techs under analysis — Table 2

| | Core services | | Financial services | | | | | Technology services | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Big tech | E-commerce | Digital consumer services# | Banking% | Credit provision | Payments | Asset management | Insurance | Cloud-based solutions* | Data analytics | Other& |
| **Alibaba (Ant Group)** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Amazon** | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |
| **Grab** | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | |
| **Jumia** | ✓ | ✓ | | ✓ | ✓ | | | | | |
| **Mercado Libre** | ✓ | | ✓ | ✓ | ✓ | ✓ | | | | |
| **Rakuten** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |

✓ Provision of financial service through big tech entity and/or in partnership with financial institutions outside the big tech group in at least one jurisdiction.

# Social networks, mobility, deliveries and media services.

% The main activity of an entity engaged in banking is taking deposits, though regulations vary across countries.

* This includes both cloud storage and cloud computing solutions.

& Other technology services include, for example, telecommunication services, navigation services and digital workplace services.

Sources: BIS (2019); Citi GPS (2018); FSB (2019a); IBF and Oliver Wyman (2020); Van der Spek and Phijffer (2020); public sources; FSI.

[12] Grab in Singapore also has a payments platform to enable users to shop online at partner websites and make their payments with GrabPay.

[13] See Synergy Research Group (2022).

## Ecosystem binders

11. **Big techs' digital platforms are designed around ecosystem binders.** These are applications and tools that integrate the entire ecosystem and facilitate and promote its use, thereby building a loyal and captive user base. Examples of ecosystem binders include super apps,[14] unique commercial identifiers, loyalty programmes, credit cards that grant discounts when purchasing products in the ecosystem, or premium services offered to (active) merchants (Table 3).

12. **By encouraging customer engagement and cross-usage of services, ecosystem binders generate data from different business segments**. For instance, the "service cross-use ratio" of Rakuten was 73.9% in June 2021, meaning that two out of three Rakuten members use two or more services on the platform.[15] Big techs also obtain data from business acquisitions as customer information is one of the main assets that is transferred. For example, Amazon obtained a large amount of data on grocery purchasing habits and preferences of consumers when it acquired Whole Foods in 2017.

Big techs – ecosystem binders — Table 3

| Big tech | Alibaba (Ant Group) | Amazon | Grab | Jumia | Mercado Libre | Rakuten |
|---|---|---|---|---|---|---|
| Super app | ✔ | ✔ | ✔ | ✔ | | ✔ |
| Loyalty programmes | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Premium services[#] | ✔ | ✔ | | | ✔ | ✔ |
| Credit cards[%] | | ✔ | ✔ | | | ✔ |
| Others[+] | | | ✔ | | | |

[#] Premium services such as faster delivery and exclusive deals for customers; and premium data analytics and upgraded storefront management tools for merchants.

[%] Credit cards in partnerships with payment services providers such as Amazon Prime Rewards Visa Signature Card, GrabPay Card, which is a prepaid Mastercard, and Rakuten Visa Card.

[+] Grab Academy, which is an online training platform available for driver-partners.

Sources: Public sources; FSI.

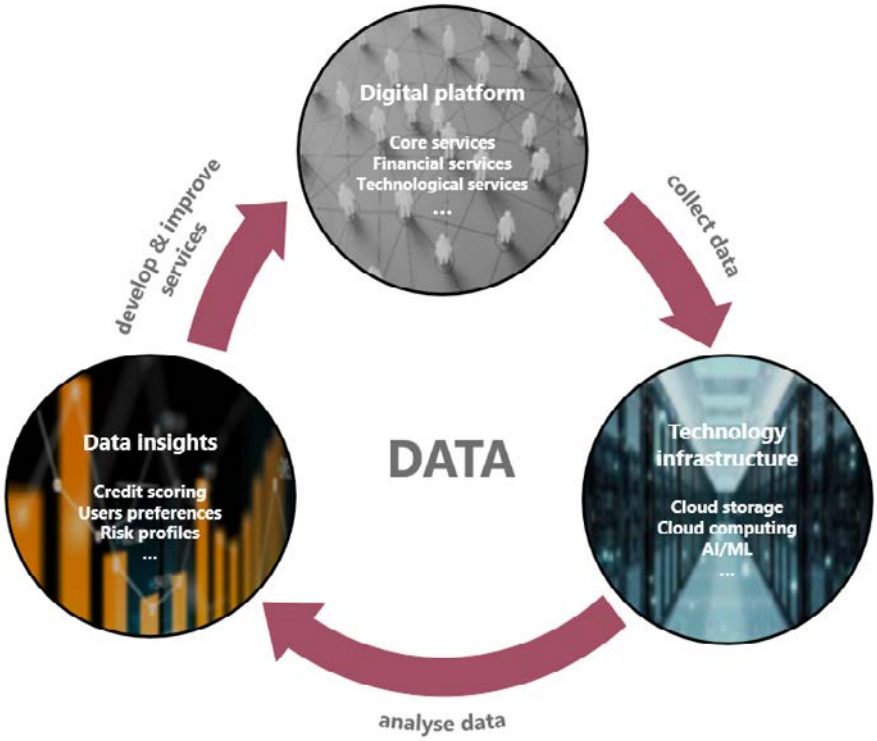
## Ongoing expansion

13. **Big tech groups can leverage the data analytics, network externalities and interwoven activities (DNA) loop to reinforce the attractiveness of their ecosystem.** Taking advantage of cutting-edge analytical and technological applications, big techs actively use their stock of client data as input to create further user activity (Graph 2). The more services a platform offers, the more attractive it is for its users, both customers and sellers. More data collected, in turn, provide a better basis for data analytics, which allow big techs to offer better and a wider range of products and services. The network externalities of big tech platforms kick in and bring about value to existing users by attracting more users and by incentivising current users to keep using the platform (BIS (2019)). Platforms can thus attain a critical mass of users and make the most of network effects.

[14] Super apps refer to mobile or web applications that aggregate most or even all financial and non-financial products and services offered by companies in a big tech group.

[15] Rakuten (2021).

Big tech's data cycle Graph 2




Source: Authors' conceptualisation.

14. **Network externalities provide incentives for big techs to both scale up and broaden their services and attain dominant positions.** As big techs enable direct interactions among a large number of users, they can quickly reach a market's tipping point and attain dominant positions. For example, Alipay's number of active users grew by 15% between 2016 and 2017 (from 450 million to 520 million users) and by 73% the following year (from 520 million to 900 million users).[16] To reach this tipping point, big tech groups implement business strategies such as penetration pricing, product differentiation or product compatibility.[17]

15. **Big techs' growth generally follows both horizontal and vertical integration strategies.** Amazon, for example, started as an online bookstore in 1994 and gradually expanded to a wide variety of sectors through organic growth and the acquisition of 13 companies between 2012 and 2020.[18] While integrating new activities, big techs look to reinforce the synergies and complementarities between their activities in pursuit of the tipping point and activate network externalities. For example, in January 2022 Grab completed the acquisition of a majority stake in Jaya Grocer, an important supermarket chain in Malaysia, to consolidate its leadership position in the online food delivery market in Southeast Asia. In December 2021, Mercado Libre acquired the Chilean payment services providers Redelcom to further enhance its digital payment tools offer for SMEs. The growth into new activities is supported by a strong customer base, brand recognition and the ability to cross-subsidise new activities.

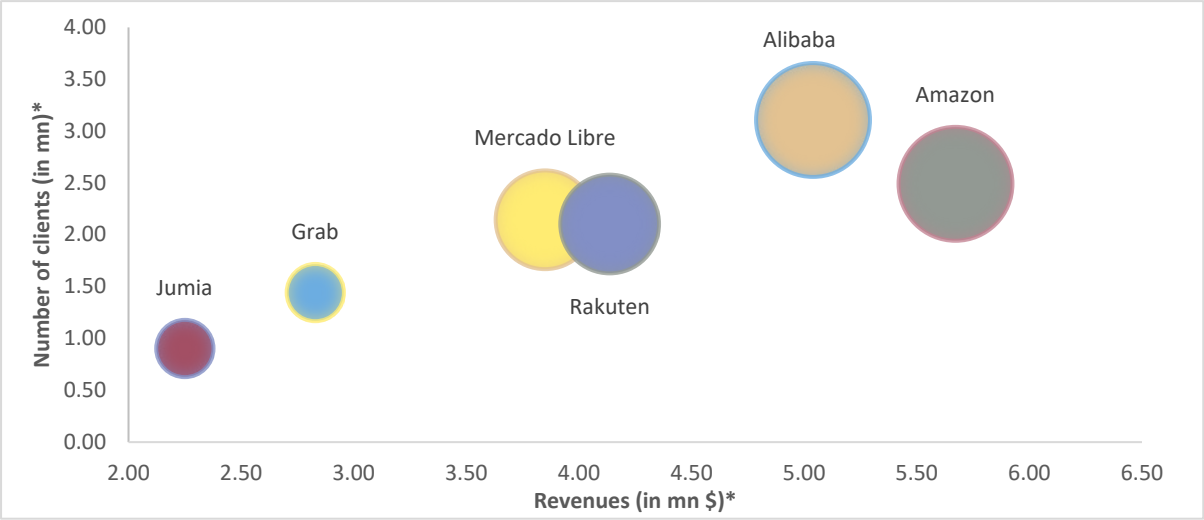
16 See Klein (2019).

17 To illustrate the product compatibility point, Amazon offers a wide range of compatible devices, such as smart home devices and Fire TV, which work with Amazon's cloud-based virtual assistant Alexa.

18 See The Washington Post (2021a). Amazon has also expanded to home security (acquisitions of Blink and Ring in 2018) and autonomous cars (acquisition of Zoox in 2021).

16. **Depending on their size and stage of growth, big techs can be described as regional or global.** Driven by strong network externalities, big techs have incentives to continuously grow beyond their core activities and home market. This drive for growth has led big techs to reach different stages in their development.[19] Alibaba and Amazon operate globally in a large number of businesses with an extended customer base. Grab, Jumia, Mercado Libre and Rakuten, in turn, tend to operate regionally in a more limited number of segments with a relatively smaller customer base but expanding towards new services (Graph 3).

Regional vs global big techs — Graph 3




Size of circles indicates the number of continents on which the platform operates. Data as of end-2021, in log scale.

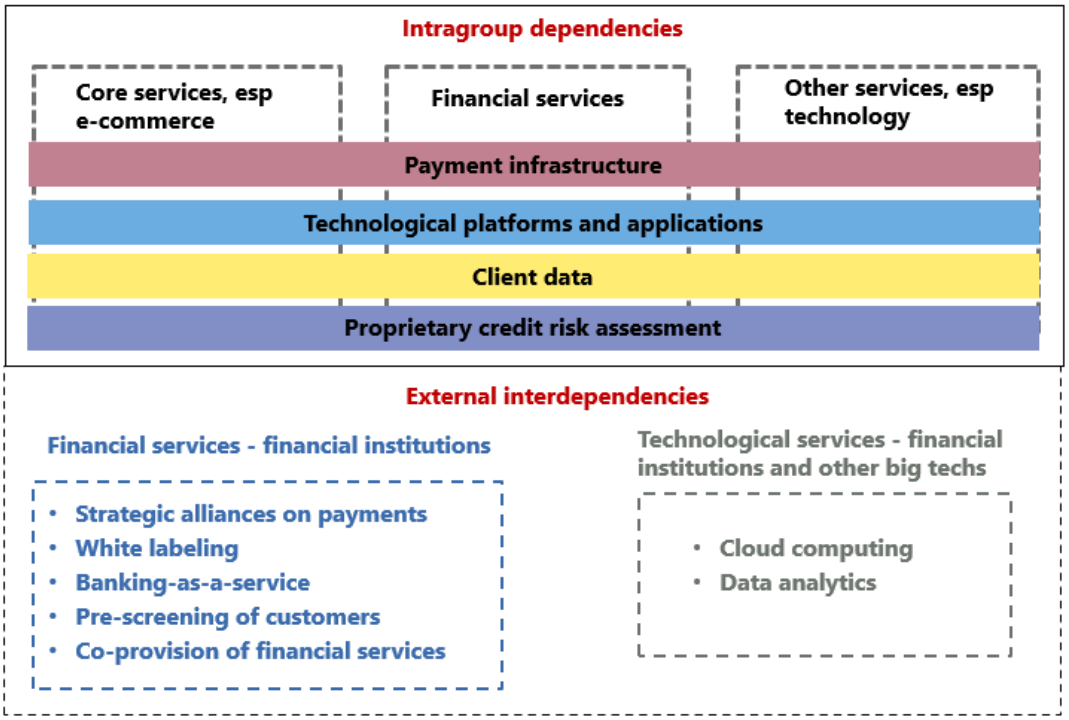
Source: Annual reports; FSI calculations.

## Internal and external interdependencies

17. **Big tech business models are characterised by strong internal and external interdependencies (Graph 4).** Intragroup dependencies arise from the common use by big tech entities of both a general payment infrastructure and technological platforms and applications. They also arise because big tech entities share data and insights derived from those data across the services they provide. External interdependencies, on the other hand, arise from partnerships of big tech entities with incumbents to provide financial services; and the provision of technology services, such as data analytics and cloud computing to other companies.

[19] All six big techs under analysis have announced in their annual reports their intent to pursue further growth in terms of ambitious investments, acquisitions and market expansion.

Big tech interdependencies Graph 4




Source: Authors' conceptualisation.

## Section 3 – Intragroup dependencies

18. **Intragroup dependencies help big techs to achieve economies of scale and scope but also exacerbate operational, reputational and contagion risks across their operations.** Digital platforms benefit from common payment and technological infrastructures that facilitate transactions and data processing across the entire ecosystem. However, an operational failure of a common technological infrastructure, such as the recent global outages of Amazon Web Services (AWS),[20] may affect the operations of the whole big tech group, including its financial business lines. Moreover, regulated financial entities that are members of a big tech group may suffer a negative impact from weaknesses or failures in the use of technologies (eg artificial intelligence (AI) / machine learning for credit risk assessments) or procedures related to data collection and processing, both of which may take place in other parts of the group.[21]

### Payment infrastructure

19. **Big tech firms' entry into financial services has commonly started with payment services, where they have reached a substantial market share in some jurisdictions.** For instance, in 2020 Alipay and Tencent accounted for more than 90% of the mobile payments market in China.[22] Similarly, Google

[20] It appears that AWS outages in 2021 affected not only third-party AWS customers but also the e-commerce business of Amazon itself. See The Washington Post (2021b) and www.globaldots.com/resources/blog/recent-aws-outages-should-you-panic.

[21] See Prenio and Yong (2021) on emerging regulatory expectations for the use of AI in the financial sector.

[22] See The Economist (2020).

Pay, Amazon Pay, and WhatsApp accounted for around 36.6% of the Unified Payments Interface (UPI) app transaction volume in India during January 2022.[23]

20. **A core aspect of big tech business models is to run easy-to-use payment systems.** Big techs' proprietary payment systems allow them to facilitate transactions across their large networks of users, to reduce frictions in their ecosystem, to eliminate fees from third-party banks or other payment processors, and to deal directly with customers' complaints. They are also crucial instruments for connecting their different business segments.

21. **Proprietary payment systems are usually embedded in one-stop digital shops enabling users to interact with products and services across the entire ecosystem**. For example, Alipay's super mobile app connects users with about 80 million merchants, over 2,000 partner financial institutions, and a wide array of everyday services. Similarly, Amazon Pay in India offers a one-stop application and a website that allows users to make utility bill payments, recharge public transportation cards, acquire insurance services, book transportation, transfer money and pay municipal taxes. A one-stop digital payment of day-to-day services is also offered by JumiaPay, but on a smaller scale.[24]

22. **Besides one-stop shop applications, some big techs offer a wide range of other on- and offline payment methods connected to the ecosystem.** For instance, Rakuten offers a suite of payment methods that are attached to a single Rakuten ID. These include online payment methods (eg the Rakuten Pay app and Rakuten Edy e-money) as well as other physical payment solutions (eg bank credit cards with special benefits if used within the ecosystem, or QR code and barcode payments). Similarly, Mercado Pago provides an e-wallet that allows users of Mercado Libre to make payments on the e-commerce platform as well as on external merchants' websites that have integrated this payment option. Additionally, it offers payment solutions for bricks-and-mortar stores through QR codes and mobile points of sale (MPOS) devices. Finally, GrabPay provides on- and offline digital payment solutions using a mobile wallet.

## Technological platforms and applications

23. **Big techs take advantage of technological advances not only through in-house development but also via investments, joint ventures and acquisitions.** This is to leverage on companies' tech talent and to take advantage of strategic positions. It is common for big techs to eventually integrate those companies in their own ecosystems under their own name. For instance, Amazon has invested in and acquired a variety of early payment fintechs such as TextPayMe, Bill Me Later, GoPago, QwikCilver, among others. Rakuten has invested in more than 60 startups that benefit from access to Rakuten networks and the interaction with the Rakuten Ecosystem. There is also increasing evidence of technological partnerships between big techs and financial institutions aimed at joint product development.[25]

24. **Big techs' ecosystems rely on common technological infrastructures.** These refer to all the physical (servers, computers, facilities, hard drives etc) and non-physical (software, applications, cloud structures, data lakes etc) elements that support the storage and transmission of data, and other operations of big techs. Global big techs' technology infrastructures are usually developed in-house, through a tech subsidiary, or obtained by means of acquisitions, investments, and partnerships. In contrast,

[23] See inc42.com/buzz/phonepe-maintains-lead-in-upi-with-49-market-share-in-jan-2022-whatsapp-at-0-02 and, on related policy developments, economictimes.indiatimes.com/tech/technology/npci-enforces-new-market-share-rules-on-upi-for-google-pay-phonepe-paytm-others/articleshow/81701508.cms.

[24] Jumia mainly offers utility bill payments, airtime recharge and transport ticketing.

[25] For instance, the partnership between the insurer Generali and Google (see Box 2 in Brits et al (2021)). Generali Italy and Google have been in a five-year strategic partnership since June 2019. The aim is to transform, innovate and adapt Generali's products and services, and attract innovative talent. New products are being developed with Google Cloud in a technology laboratory in Italy.

regionally focused big techs' infrastructures are usually built upon third-party technology foundations (such as public clouds) and open source resources. For instance, while Alibaba or Amazon have a technology business arm within the group, regional big techs such as Mercado Libre, Grab and Jumia depend on third-party technology providers such as AWS, Alibaba Cloud, Teradata and IBM.

25. **Global big techs commonly leverage their own cloud computing capabilities to operate other business segments within the group.** For instance, Ant and its parent, Alibaba, entered into a Cloud Services Framework Agreement, whereby Ant obtains cloud computing services, cloud-related products and other services from Alibaba's subsidiaries and associates. Similarly, Amazon's retail businesses fully migrated to its AWS subsidiary's infrastructure in 2011.[26]

26. **Different entities within a big tech group use and share other computer applications and analytical tools for managing different activities.** For instance, Ant and Alibaba entered into an SME Loan Software System Use and Service Agreement that allows Ant to use Alibaba's software systems to conduct its microfinancing business for an annual fee. Similarly, Mercado Libre's data architecture leverages Alation and Tableau[27] to provide their employees with self-service tools for processing, analysing and visualising customer data from different business segments. In the case of Rakuten, deep learning technology developed by its AI platform programme allows its staff to analyse client behaviour across its various business segments.[28]

## Personal data

27. **Big techs' business models heavily rely upon sharing client data across their business segments to improve or expand their offerings.** Public privacy notices and annual reports suggest that big techs commonly share client data within the group without much friction. For instance, public statements from Rakuten, Mercado Libre and Grab state that they usually share data with subsidiaries and affiliates.[29] In the case of Alibaba and Ant, which are separate legal entities, data-sharing agreements are common which allow the sharing of certain data collected or generated within each business under the governance framework provided for in the agreement.[30]

28. **Depending on their specific business model, big techs collect different types of data and use them for different purposes.** Big techs collect a wide range of information on their customers. Data are then analysed and used to improve or tailor products and services, or sold to third parties. According to privacy notices, big techs use customers' data also for account administration, detection of abnormal activity, offering of promotions, rewards and subscriptions, detecting and preventing financial crimes, regulatory compliance and risk assessment (Graph 5).

[26] See Jenkins (2011).

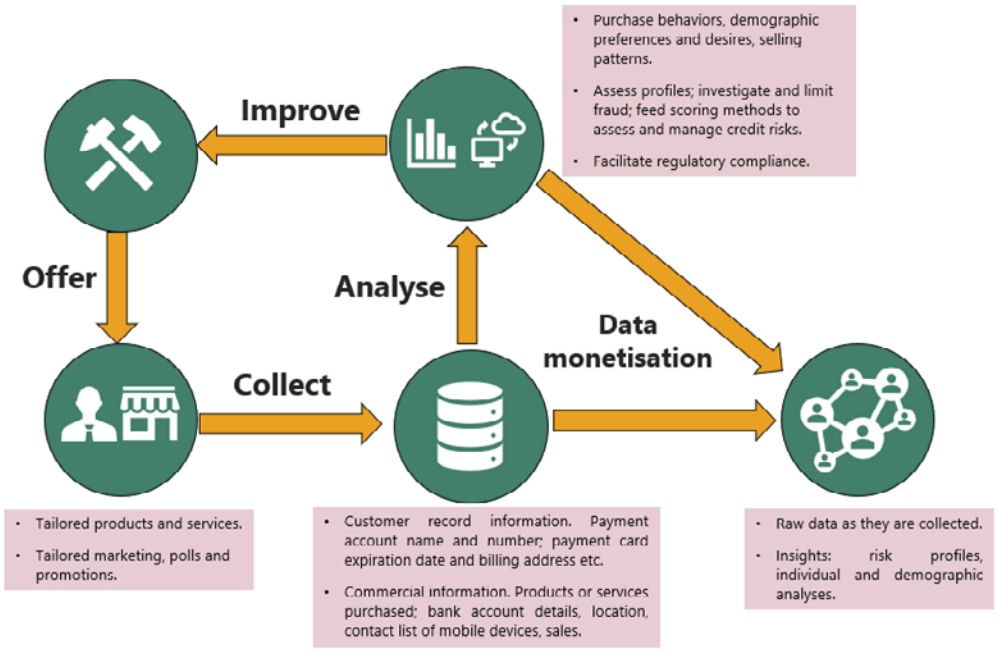
[27] Alation and Tableau are computer applications focused on data management, analytics, and governance.

[28] See Rakuten Today (2019).

[29] See privacy notices from Rakuten (corp.rakuten.co.jp/privacy/en/link.html), Mercado Libre (global-selling.mercadolibre.com/privacy/privacy-notice) and Grab (grab.com/sg/terms-policies/privacy-notice).

[30] See Alibaba Group Holding Limited (2020).

Common data usage by big techs Graph 5




Source: Authors' conceptualisation.

## Proprietary credit risk assessment

29. **Several big techs have developed proprietary credit scoring systems serving all their business segments.** Public information on all big techs under analysis suggests that these systems are used by both financial and non-financial companies within big tech groups. For instance, Ant's credit scoring system, which consists of more than 100 models, assesses customer profiles to produce insights into the creditworthiness of potential borrowers that allow both Ant and Alibaba to make lending decisions.[31] In the case of Mercado Libre, according to its 10-K disclosures, it uses an internally developed risk model with e-commerce data as input. This model calculates a credit quality indicator that helps predict merchants' and/or buyers' ability to repay when seeking a loan under the Mercado Credito solution.[32]

30. **Big techs leverage alternative data and sophisticated artificial intelligence-based tools as part of their credit scoring systems.** These systems can identify eligible potential customers who might not qualify for credit on the basis of traditional credit risk models used by financial institutions. This is possible because big tech models not only analyse the credit history of customers but also past transactions and digital behaviour in their ecosystems – the so-called digital footprint.[33] Jumia, for

[31] In September 2021, it was reported that Chinese authorities requested that Ant: (i) establish a new separate entity for its lending business (Huabei and Jiebei); (ii) remove any lending functionality from its payment app and create a separate app for this purpose; and (iii) transfer proprietary data used for its lending decisions to a separate credit scoring entity. This new partly state-owned entity was reported to apply for a consumer credit scoring license. See www.ft.com/content/01b7c7ca-71ad-4baa-bddf-a4d5e65c5d79.

[32] In some cases, credit scoring systems are also used by merchants or partners that operate in the big tech ecosystem. For instance, Alibaba's partners rely on Zhima Credit score system to assess consumers' trustworthiness and offer deposit-free services to those clients with eligible Zhima Credit score across a variety of daily life use cases including hotel booking, ride sharing and car rentals.

[33] See Berg et al (2018).

example, uses a diverse set of data it collects on transactions on its platform as basis for the development of its credit system, fraud scoring tool and risk monitoring processes. Overall, the advantages of big techs' credit scoring systems have become important for their service offerings, and therefore their profitability.

## Section 4 – External interconnections

31. **Big techs and financial institutions offer financial products and services through a variety of partnerships.** These range from performing front-end functions to co-providing financial products and services.[34] The lack of transparency around these arrangements makes it unclear whether they provide incentives to increase risk-taking through, for instance, riskier lending (FSB (2022), IMF (2022)). However, it is clear that these arrangements create a wider surface for cyber attacks and other criminal activities. Moreover, when the financial services value chain is spread across different players, it is more difficult to identify responsibilities for failures in protecting consumers' interests (Feyen et al (2021)). In this context, a failure in the operation of a big tech could negatively impact the reputation of its partner financial institution.

32. **Big techs' technological superiority underpins their role as a critical third-party service provider for financial institutions and other big techs.** Financial institutions significantly rely on technology services provided by big techs such as cloud computing and data analytics. The analysis in this paper confirms this dependence and finds ground to argue that regional big techs also heavily rely on technology services by global big techs. As a result of big techs' investment in cutting-edge technology, the financial system's dependence on a few critical service providers is likely to increase going forward. While this dependence might increase the resilience of individual financial institutions and could be cost-effective for smaller ones, it would exacerbate system-wide operational and concentration risks in case big techs were to experience significant disruptions.[35] These disruptions might be amplified through the interconnections between global and regional big techs and could have a broader impact on the global economy.

### Partnerships between big techs and financial institutions

33. **Big techs enter into partnerships with financial institutions and other large companies to facilitate payments in their ecosystem.** While global big techs largely rely on their own proprietary payments infrastructure to achieve this objective, they also enter into different types of arrangements with myriad financial institutions and payment companies to expand their activities to other regions and facilitate cross-border payments. This partnership strategy seems more evident in the case of regional big techs. For instance, Jumia announced a partnership with the National Bank of Egypt in August 2021 to offer business payment services for third-party merchants on the Jumia e-commerce marketplace in Egypt. Also, Grab entered into a partnership with Mastercard to develop its GrabPay Card and make it available both online and in stores globally.

[34] There is also evidence of increasing interconnectedness between big techs and financial market infrastructures. According to FSB (2022), payment systems and investment services developed and operated by big techs could have increasing exposures and potentially contagion effects to financial market infrastructures and other participants in the financial ecosystem. A couple of examples are highlighted by IMF (2022): Alipay and WeChat Pay are interconnected with NetsUnion Clearing Corporation in China, and Google Pay has a direct connection with the Unified Payments Interface and Immediate Payment Service in India.

[35] Standard-setting bodies and financial authorities have been following these developments and highlighted some common concerns that may arise from third-party dependencies (FSB). These include: (i) operational incidents that may result in outages and data breaches; (ii) a reduction in the ability of financial institutions and authorities to properly assess compliance and risk due to contractual limitations on rights of access, audit and information; and (iii) concentrations that may result in systemic threats stemming from big techs' large-scale operational failures or insolvency.

34. **Through white labelling arrangements, big techs act as the front-end customer interface offering financial products and services provided by financial institutions.** Under these arrangements, big techs typically provide the customer access interface (under its own name) for financial products or services that are issued and managed by financial institutions. For instance, while Rakuten Card is marketed and offered by Rakuten in the United States, the card is issued and managed by Synchrony Bank.[36] Another example is Mercado Fondo in Argentina, an investment fund offered by Mercado Libre but administered by a financial institution that also acts as custodian.[37] Yet another example is Apple Card, a credit card created by Apple and issued and managed by Goldman Sachs.[38]

35. **Big techs and financial institutions also engage in banking-as-a-service (BaaS) partnerships to integrate financial services from different providers into a single platform.** Through BaaS arrangements, big techs offer various financial institutions' products and services relying on application programming interfaces (APIs). These arrangements allow big techs to integrate into their e-commerce platforms, for example, different payment methods (eg PayPal, Google Pay, Mercado Pago, Alipay) or a variety of credit offerings, as in the case of buy-now-pay-later partnerships with AliExpress and Klarna. BaaS arrangements also include super apps that bring together various financial institutions' products and services using a single platform such as Alipay or WeChat in China and Amazon Pay in India.

36. **Big techs expand the digital sales channels of partner financial institutions by offering their products to eligible customers.** Financial institutions benefit from combining the pre-screening insights generated by big techs with their own data to make formal approvals and/or underwritings. This is the case of Amazon's partnerships with Marcus by Goldman Sachs in the US and ING in Germany. For Marcus by Goldman Sachs, Amazon regularly evaluates merchants' growing sales and customer satisfaction, among other metrics, to identify eligible customers for business financing options to be provided at Marcus' discretion. For ING Germany, Amazon acts as a broker of loan proposals to eligible businesses who sell their goods through its portal and directs them to ING's website for submitting their credit application.[39]

37. **Big techs share their clients' data with financial institutions to be used as inputs to their risk management assessments.** Although there is limited public information about this type of partnership, the arrangement between HSBC and Cainiao Network Technology (the logistics arm of Alibaba Group) provides a relevant example. Under this arrangement, credit is offered to online merchants on Chinese shopping site Tmall. Applicants do not need to submit any documents and no collateral is required. However, Cainiao customers must accept sharing business-related data with HSBC such as balance sheet and inventory information.[40] Another example would be the partnership between Amazon and Marcus by Goldman Sachs to offer credit lines to merchants. Amazon provides information on customer behaviour to Marcus, which is responsible for the credit underwriting.[41]

38. **Big techs and financial institutions also enter into arrangements to originate and/or distribute lending and insurance financial products.** Under these partnerships, big techs actively

[36] See rakutencard.syf.com/login/.

[37] See www.mercadolibre.com.ar/institucional/hacemos/mercado-fondo.

[38] See support.apple.com/es-es/HT209218. Apple Card is marketed by Apple, which also provides an e-wallet app and other useful tools for customers. In turn, its partner Goldman Sachs is in charge of approving the customer's card application using its own credit scoring system and is responsible for settling payments and implementing the necessary risk management framework. In June 2022, it was reported that Apple intends to offer a new buy now, pay later credit product – Apple Pay Later. According to the Financial Times (2022), Apple plans to extend credit through a wholly owned subsidiary, Apple Financing LLC, which would be handling the underwriting and lending, with Goldman Sachs enabling access to the network of Mastercard.

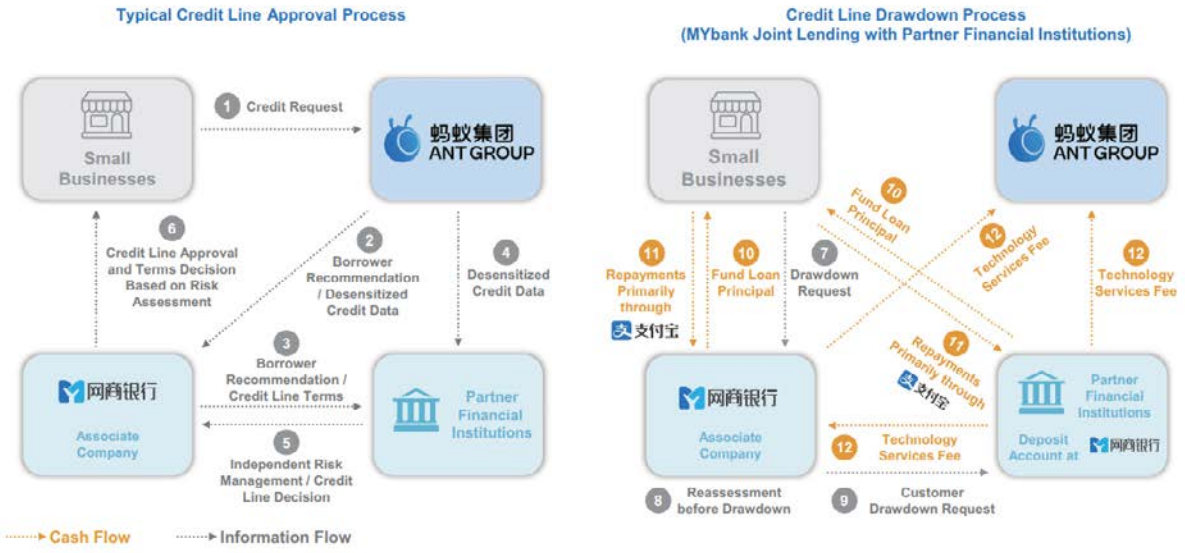
[39] See www.ing.com/Newsroom/News/ING-in-Germany-and-Amazon-join-forces-in-SME-lending.htm.

[40] See www.about.hsbc.com.hk/-/media/hong-kong/en/news-and-media/200319-hsbc-launches-innovative-digital-trade-finance-solution-en.pdf.

[41] See Congressional Research Service (2022).

participate as product designer, debt collector and/or risk manager, among other activities. These arrangements are more common for big techs in China than in other regions. Ant Group, for instance, partnered with approximately 100 banks to provide credit (as of June 2020). About 98% of the loans originated on Ant's platform were underwritten or securitised by partner financial institutions.[42] For its services, Ant receives service fees calculated as a percentage of the interest income that financial institutions earn. Graph 6 shows the process through which Ant and MyBank, an online bank in which Ant holds a minority stake of 30%, provide financial services.

Ant Group's joint lending process — Graph 6




Source: ANT Group (2020).

## Reliance on technology services provided by big techs

39. **As part of their digitisation strategy, financial institutions have come to heavily rely on cloud computing and data analytics services from big techs.** Cloud-based solutions allow financial institutions to increase productivity and enhance their customers' experience while reducing operating costs. A survey among financial industry decision-makers across North America, Europe and Asia-Pacific found that 83% of respondents are already using some form of public cloud.[43] The market for cloud computing services is highly concentrated. Latest estimates indicate that the top four providers (ie Amazon Web Services, Microsoft Azure, Google Cloud and Alibaba Cloud) control around 70% of the global market across all sectors.[44]

40. **Financial institutions' cloud adoption, and hence their dependence on big techs providing these services, is likely to increase going forward.** Cloud adoption in the financial sector is driven by several factors such as: (i) the greater use of big data and artificial intelligence applications; (ii) increased opportunities for business activities to be moved to the cloud (eg regulatory compliance, fraud detection

[42] In the meantime, draft rules for online lending were issued which require internet companies (including big techs) to fund 30% of the value of the loans they distribute (thereby limiting the funding provided by banks and other firms to 70%).

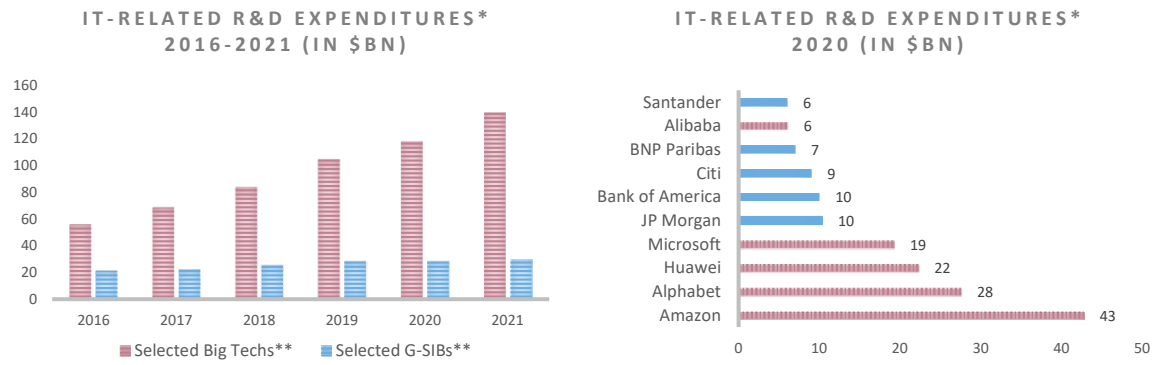
[43] The survey was commissioned by Google Cloud and was conducted online from 7 December 2020 to 4 January 2021. A total of 1,363 risk/compliance and IT leaders worldwide were surveyed. See Google Cloud 2021. However, According to Fortune Business Insights: Cloud Computing Market Size, Share & Industry Growth (fortunebusinessinsights.com), the financial sector is estimated to represent around 16% of the global cloud computing market.

[44] See Synergy Research Group (2022).

and transaction monitoring); and (iii) state-of-the-art security frameworks provided by leading cloud providers. According to the survey cited above, financial institutions that were using on-premises technological infrastructure at the end of 2020 had plans to switch, on average, 40% of their business operations to public cloud during 2021.[45] Consequently, public cloud spending is envisaged to exceed 45% of all enterprise IT expenditure by 2026, up from less than 17% in 2021;[46] and the global cloud market is projected to grow from $250 billion in 2021 to close to $800 billion in 2027.[47]

41. **Big techs' technological superiority underpins their role as critical service provider of financial institutions.** Although financial institutions have launched efforts to take full advantage of technological innovations, they are held back by IT infrastructure that has developed over many years and may not always live up to more demanding standards. Big techs, in contrast, are unburdened by legacy systems, making it easier for them to embrace innovations.[48] But they also spend more on IT-related research and development (R&D) than the largest banks. The left-hand panel of Graph 7 shows that big tech IT-related R&D expenditure in the period 2016–21 was 3–4.5 times higher than the one by global systemically important banks (G-SIBs). The panel also shows that big tech R&D expenditure has consistently increased over time by on average close to 20% in 2016–19 and 13% in 2020–21. In comparison, G-SIB expenditure grew during the same period by around 10% and 2.5%, respectively. The right-hand panel of Graph 7 shows that big techs spent between two to four times more in IT-related R&D in 2020 in comparison with G-SIBs. Moreover, this expenditure appears to be continuously increasing. For instance, Amazon's and Alibaba's R&D investment increased by around 30% between 2020 and 2021.

Big tech vs G-SIB technological investments — Graph 7




* Reported IT-related expenses correspond to R&D expenses for big tech companies and technology and communication expenses for financial institutions.

** Selected big techs include Amazon, Alibaba, Alphabet, Huawei, Microsoft. Selected G-SIBs include JP Morgan Chase, Citigroup, Deutsche Bank, Goldman Sachs and HSBC.

Sources: JP Morgan, annual reports; FSI calculations.

42. **Big techs' technological investments are driven by their emphasis on data privacy and cyber security.** Over the past six years, leading US-based big techs[49] have invested in more than 50 cyber security companies to acquire advanced tools and capabilities on threat detection and data protection (CB

[45] See Google Cloud (2021). In addition, those who rely on some form of public cloud (but haven't transitioned all of their workloads fully) expect to move, on average, another 27% of their workloads to the public cloud in the next 12 months.

[46] See Gartner (2021a).

[47] See Fortune Business Insights (2021).

[48] As one example, Rakuten Mobile built the world's first end-to-end fully virtualised mobile network in only 18 months (Rakuten (2020)).

[49] This refers to Facebook, Amazon, Microsoft and Google/Alphabet.

Insights (2022)).[50] The main rationale behind these investments is not only client trust but also complying with the increasing regulatory expectations around handling a large volume, variety and velocity of personal data.[51] Offering best-in-class capabilities in this domain is attractive for existing and prospective customers and, therefore, demand for robust cyber security solutions is expected to grow, particularly if they are already integrated into cloud platforms. This line of business, in turn, provides an important source of constant revenue growth in the long run.

43. **Big techs' investments in emerging technologies such as quantum computing are likely to deepen their critical role in the financial system.** While this technology is at an early stage, it has huge promise. Quantum computers may, for example, solve many tasks exponentially faster than classical computers, opening a wide array of new possibilities for advanced algorithms.[52] As part of these developments, Amazon has launched a quantum cloud service and has started to develop its own quantum hardware.[53] Moreover, Google has committed several billions of dollars to build a functional quantum computer by 2029.[54] Experts envisage that few companies will be able to build or own quantum computers in the near term and see a cloud computing-style model emerging where companies rent access to quantum machines hosted by a relatively small number of specialist providers (Ruane et al (2022)).

44. **In addition to financial institutions, regional big techs tend to rely on technological infrastructure and analytical tools developed by global big techs.** As described in Graph 8, Jumia, Mercado Libre and Rakuten rely on AWS solutions for storage and data processing. Grab has adopted a multi-cloud strategy, using both AWS and Microsoft Azure for cloud services such as data computing, machine learning and artificial intelligence. Following last year's merger between Go-Jek[55] and Tokopedia[56] to form the GoTo Group, the largest digital ecosystem in Indonesia, it chose Google Cloud as its main cloud service provider.[57] Graph 8 also offers an illustrative example of how regional big techs are interconnected with selected G-SIBs through the cloud services provided by global big techs.

[50] On 8 March 2022, Mandiant, a cyber security firm, announced its acquisition by Google for $5.4 billion. This is the second biggest acquisition in Google's history.

[51] According to Gartner (2020b), by 2023 65% of the world's population will have their personal data covered under modern privacy regulations, up from 10% in 2020. Gartner defines "modern privacy laws" as those introduced in the same vein as the European General Data Protection Regulation.

[52] See Quantum Computing for Business Leaders by Jonathan Ruane, Andrew McAfee, and William D. Oliver at Harvard Business Review, January-February 2022.

[53] Microsoft has also started to offer access to quantum computers and to develop its own quantum hardware. See CB Insights (2021).

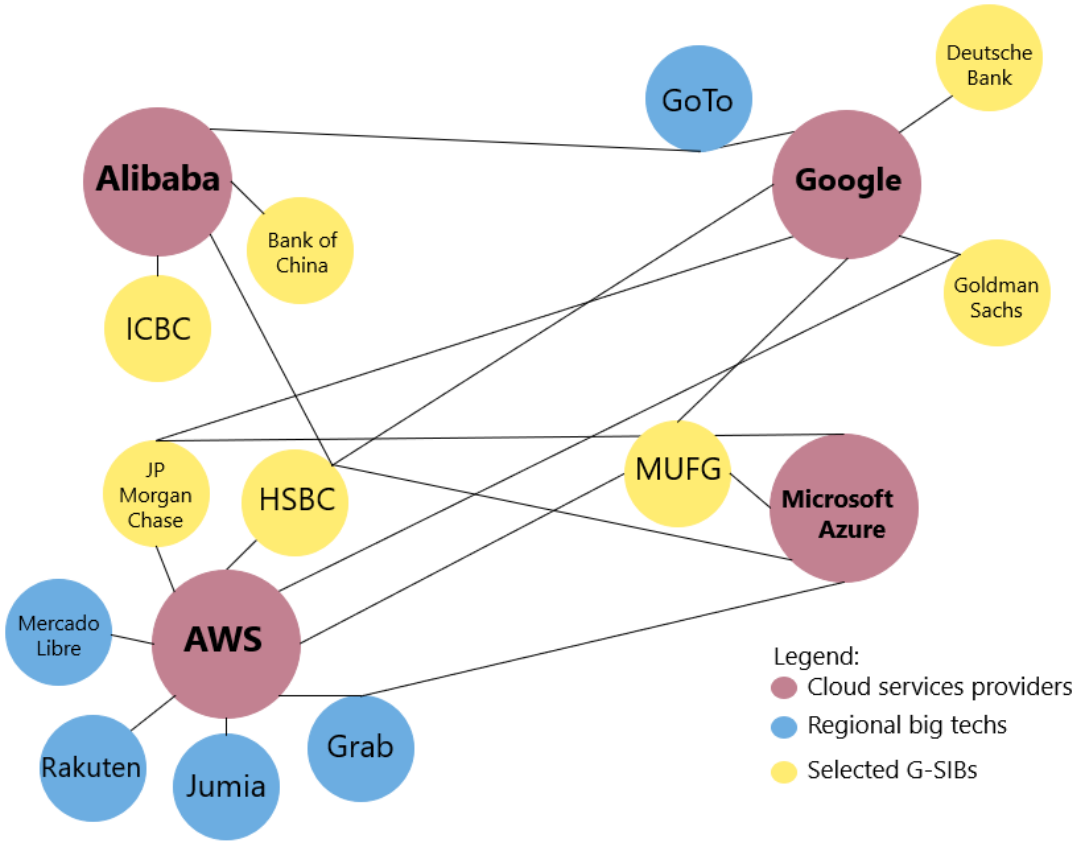
[54] This commitment was made by Google in May 2021 and includes a new campus for AI in Santa Barbara that will house hundreds of quantum dedicated employees, a quantum data centre, research labs and quantum processor chip fabrication facilities.

[55] Indonesian mobility platform that relied on Google Cloud and its machine learning technology to take advantage of customer data and develop new solutions such as dynamic pricing.

[56] Indonesian e-commerce platform that used Alibaba Cloud, in particular its artificial intelligence solutions, to enhance its customers' experience.

[57] Also, Mambu, a German technology company for banking, decided to store its code base on AWS, making it quickly and globally available to their customers. This implies that Mambu's clients, mostly financial institutions, are also reliant on AWS. For example, OakNorth, a bank based in the United Kingdom, is Mambu's client and hosted, de facto, on AWS. To mitigate this dependence on global big techs, some regional big techs also build their technological infrastructures upon third-party technology foundations (such as public clouds) and open source resources.

Reliance on technology services provided by big techs Graph 8




Source: Authors' conceptualisation. Illustrative example of interconnections between big techs and financial institutions. Proximity to a cloud provider does not indicate more or less reliance.

## Section 5 – Policy considerations for financial sector regulation and supervision

45. **Addressing the risks created by strong intragroup dependencies among different big tech entities requires a big tech group to be treated as a unit.** Strong intragroup dependencies in big tech operations (ie common payment infrastructure and technological solutions; data-sharing arrangements; and proprietary risk assessment system) weld together activities that are provided by different entities within big tech groups and therefore increase the potential for difficulties at one or more big tech activities to spill over to the entire group. These difficulties may affect not only the inner workings of big techs but also their external customers, especially in the presence of considerable external interdependencies. Two significant outages of big tech services in 2021 substantiate the argument that these operational vulnerabilities are not merely a theoretical consideration.[58]

46. **Growing reliance by a large number of financial institutions on technology services provided by a small number of big techs makes the continuity of those services systemically relevant.** This dependency is forming single points of failure, and hence creating new forms of concentration risk at the technology services level.[59] This type of concentration risk is particularly evident in the cloud services market, where four big techs control close to two thirds of the global market for cloud computing. Because there are no readily available substitutes or infrastructures for these services, a disruption in one of these big techs could have systemic implications for the financial system.[60] Therefore, the need for big techs to implement best-in-class operational resilience and cyber security frameworks is an imperative to mitigate financial stability risks.[61]

47. **Partnerships in providing financial services have the potential to exacerbate operational, reputational and consumer protection risks as well as moral hazard issues.** When financial services are delivered through various forms of cooperation, big techs typically occupy a position between the financial institution and the customer. As such, they only perform part of the service, and the resulting fragmentation of the value chain may lead to the following vulnerabilities:[62]

- **Information and communications technology (ICT) and cyber risks.** Big techs are an attractive target for cyber criminals given the personal and transactional data that they store. They are also highly interconnected – either through the payment systems in which they participate, their partnerships with financial institutions, their role as third-party service providers or the products and services they offer to the larger public. These multiple points of contact with outside parties could make big tech entities vulnerable, and could be used as entry points for attacks. Overall, ICT and cyber risks can exacerbate risks in relation to the operational resilience and business continuity of big techs.
- **Reputational risk.** Weaknesses or failures in the operations of a big tech could negatively impact the reputation of its partner financial institutions. This could materialise as eg mis-selling

[58] On Facebook, see www.kentik.com/blog/facebooks-historic-outage-explained/; on AWS, see www.ft.com/content/6eff4cae-5df7-4746-a068-d4f6a18ba285 and aws.amazon.com/message/12721/.

[59] In the US, the Federal Trade Commission Chair noted in a recent submission that "Allowing Big Tech firms to expand into payments and financial services also raises concerns about Big Tech functioning as a single point of failure, in which a problem that affects a consumer in one domain can have outsized ramifications across other seemingly separate domains that are connected only through the centralization of Big Tech infrastructure" (Khan (2021)). See also Feyen et al (2021).

[60] See Asensio et al (2022) and Danielsson and Macrae (2020).

[61] While "traditional" financial risks are not a material source of concern at this time, this could change and deserves continuous monitoring.

[62] This may also blur the boundaries between supervised and non-supervised entities. See Brits et al (2021).

practices, violations or changes of data privacy standards,[63] algorithmic biases that lead to unethical discrimination of big tech customers or issues related to the abuse of market power.

- **Consumer protection risks.** When the financial services value chain is spread across different players, or when financial products are embedded into other activities or offered as bundles of related digital services, it is more difficult to identify responsibilities for failures in protecting consumer interests.[64]
- **Moral hazard.** When incentives are not aligned between a big tech and its partners, partnership arrangements could generate excessive risk-taking behaviour to the detriment of the financial institutions involved.[65]

48. **The activities of big techs and financial institutions are increasingly intertwined, and the resulting risks, particularly the elevated operational exposures, create potential financial stability vulnerabilities.** Due to meaningful external interconnections between big tech activities and the financial system (ie partnerships in the provision of financial services and financial institutions' reliance on big tech's cutting-edge technology), significant disruptions in big tech operations could have a substantive impact on the functioning of the financial system. In other words, higher operational risks have the potential to translate into higher financial stability risks.

49. **Big techs' operations in financial services are regulated on the basis of sectoral regulatory regimes.** At present, there is currently no specific (ie direct financial) regulatory treatment of big techs operating in finance. This means that big techs are treated like any other commercial group, and the applicable financial regulatory treatment depends on the type of financial activities they are engaged in, such as banking, extending credit or transmitting payments; and on the modalities under which they provide them (Table 4).[66] When a big tech entity provides its financial services in collaboration with other financial institutions, it will normally not need any licence because its partners will typically meet the regulatory requirements. On the other hand, in case a big tech entity is licensed to perform a regulated financial activity itself, it faces a body of regulatory requirements attached to that licence under sectoral financial regulations. These requirements are aligned, in principle, with those imposed on other market participants,[67] and determine the regulatory perimeter and supervisory oversight.

[63] One example is the Facebook-Cambridge Analytica data scandal; another is the refusal by WhatsApp users to agree to new data terms and conditions enforced by its parent, Facebook/Meta. See www.theguardian.com/technology/2021/jan/24/whatsapp-loses-millions-of-users-after-terms-update.

[64] In general, consumer protection risks may be even harder to detect if services are provided across borders, or where there is a lack of appropriate disclosures of how services are provided. See Feyen et al (2021).

[65] This principal-agent problem may be particularly acute when big techs only charge transaction fees to their partners without bearing any meaningful share of the resulting risks, for example in lending arrangements. See also IMF (2022).

[66] See also Crisanto et al (2021a) and Zamil and Lawson (2022).

[67] Carstens et al (2021) and Restoy (2021).

Licences held by big tech companies in selected jurisdictions

Table 4

| | Licences and market presence | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Banking | | | Credit | | | Payments | | | Securities | | | Insurance | | | Other | | |
| Licence held | L | P | B | L | P | B | L | P | B | L | P | B | L | P | B | L | P | B |
| Amazon | | | | | ✓ | | | ✓ | | ✓ | | | | ✓ | | | | |
| Ant Group | ✓* | | | | | ✓ | | | ✓ | | ✓ | | ✓ | | | | | |
| Grab | ✓ | | | | | ✓ | | | ✓ | ✓ | | | | ✓ | | | ✓ | |
| Jumia | | | | | | ✓ | | | ✓ | | | | | | | | | |
| Mercado Libre | | | | | | ✓ | ✓ | | | | ✓ | | | | | ✓ | | |
| Rakuten | ✓ | | | ✓ | | | ✓ | | | ✓ | | | ✓ | | | ✓ | | |

* In China, shareholding of big tech in banks is below 50%.

L = big tech has entity within group that holds financial licence in respective sector. P = market presence in partnership or joint venture with other financial institutions. B = big tech offers financial services both through partnership or joint venture with other financial institutions and has entity within group that holds financial licence.

Jurisdictions include Brazil, China, the European Union, Hong Kong SAR, Namibia, Singapore, the United Kingdom and the United States.

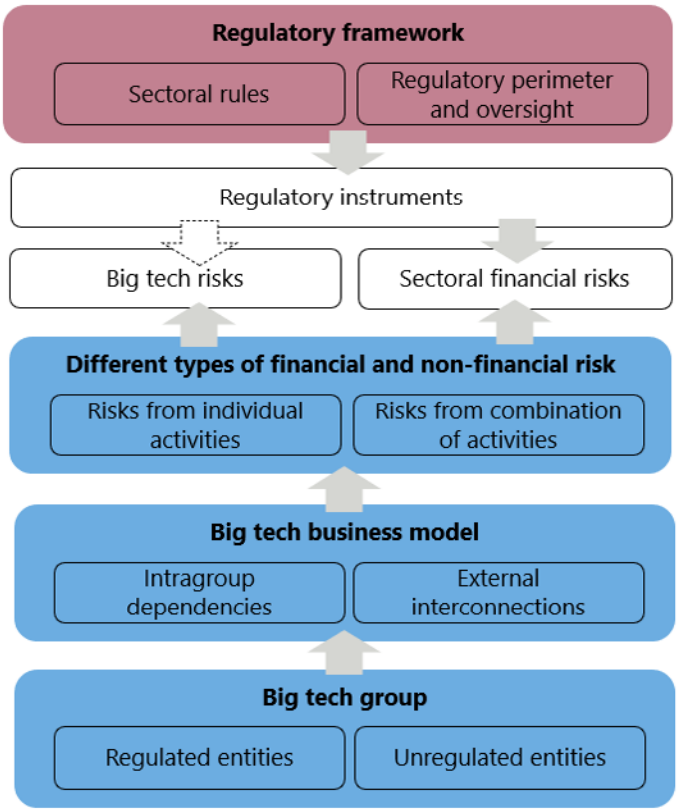
The analysis excludes cases in which payments are made and/or credit is extended for purchasing products and services exclusively within the platform.

Sources: Annual reports; Crisanto et al (2021a); public sources.

50. **The regulatory frameworks for different financial sectors were not formulated with large interconnected digital platform companies in mind.** The intermingling of financial and non-financial operations creates strong intragroup dependencies and external interconnections. Yet regulatory instruments currently available under sectoral frameworks were not designed to mitigate the risks created by these inherent features of big tech business models (Graph 9). They were designed to address the primary supervisory concerns in each sector, be it the protection of depositors, policyholders or investors; and their design had to be responsive to the main risk drivers in each sector.[68] It is therefore not surprising that risks related to interdependencies are not fully captured under sectoral regulations, not least because there is no oversight of the ultimate parent of a big tech group that bears overall responsibility for the group's financial and commercial activities and how they are interconnected.

[68] For example, insurance supervisors have historically been primarily concerned with the liability side of the balance sheet as the main source of risk; banking regulators with the asset side; and securities supervisors with the ability of securities firms to repay promptly all liabilities at any time (Gruson (2005)). See also Table 5 in Dierick (2004).

Juxtaposition of sectoral regulations and big tech risks Graph 9




Source: Authors' conceptualisation.

51. **Big tech risks stemming from interdependencies justify the development of specific entity-based rules for big tech operations in the financial sector.** In the context of big techs, risks emerge not only from the provision of a particular service, but also from the combination of all financial and non-financial activities they perform.[69] This combination, fuelled by the strong interdependencies described above, creates risks beyond the sum of those associated with each of the activities.[70] A few jurisdictions have started to insert entity-based rules in their regulatory framework to cope with selected risks presented by big techs. Several policy initiatives have emerged recently, mostly in the area of competition but also in data protection, conduct of business, operational resilience and financial stability.[71] New powers under these frameworks allow authorities to directly address some of the risks big techs pose, as is the case eg under the financial holding companies (FHC) regime in China.

52. **To effectively foster operational resilience and preserve financial stability, it appears essential that such entity-based rules comprehensively address risks related to interdependences.**[72] Additional regulatory measures for big techs should: (i) preferably follow an entity-based approach and be applied at the group level;[73] (ii) combine group-wide requirements imposed on

69 See Restoy (2019).

70 In the context of interdependencies, it appears that these are currently mainly risks to operational resilience and not so much traditional financial risks.

71 See Crisanto et al (2021b) and Restoy (2022).

72 See Restoy (2021) and Carstens et al (2021).

73 Applying requirements at the level of the legal entity carrying out the activity (ie at the solo level) would probably not be effective to address risks from interdependencies.

the parent company by home authorities with requirements applicable at the level of the legal entity active in a given jurisdiction imposed by host authorities – a description of an enhanced cross-border supervisory approach is provided in IMF (2022) and an analysis of some features of a potential regulatory framework for big techs is offered in Ehrentraud et al (forthcoming); and (iii) aim at strengthening the resilience of financial institutions that are members of a big tech group, and – indirectly – those outside big techs that partner with or substantially rely on services provided by big techs.[74] In addition, enhanced dialogue and new forms of cooperation between financial authorities, competition commissions and data governance regulators would be essential components of improved institutional coordination.

53. **As the discussion on specific rules for big techs is gaining momentum, authorities are searching for interim solutions.** The time needed for sound policymaking contrasts with the speed with which big techs move. Meanwhile, financial authorities may wonder what they can do now to deal with those big tech challenges that fall within their mandate. They may, as a matter of practicality, start with what they have. For authorities, this would mean focusing on regulated financial entities, and using them as a lever to counter potential financial stability risks.

- **For regulated financial entities that are members of big tech groups, authorities may wish to assess whether they have a clear picture of the risks stemming from interdependencies.** They may take the following steps to enhance their understanding. First, assess how regulated entities that are part of big tech groups are embedded in their group structure. Second, ask whether there is sufficient information on the activities and risk profile of the regulated entities, particularly against the backdrop of their function in the big tech ecosystem.[75] Third, assess potential risk transmission channels and whether there are any unaccounted risks from the wider group that affect them. If there are, analyse whether these could jeopardise the financial condition or operational resilience of regulated entities. Lastly, based on this assessment, enter into a structured supervisory dialogue with the examined entities to discuss the findings and potential risk mitigants.
- **For all regulated financial entities, authorities may wish to assess whether there is a need to strengthen digital operational resilience.** The universe for such an assessment would include regulated institutions that: (i) are members of a big tech group; (ii) play an active part in a big tech ecosystem and/or provide services in collaboration with big techs; or (iii) depend on big tech services. The ability of these entities to withstand and mitigate threats and potentially severe disruptive events could be scrutinised on the basis of their compliance with outsourcing and risk management rules. This would include an assessment of their risk management practices related to third-party risks and, where possible, fourth-party relationships and concentration risk exposures.[76] It would also include assessing regulated entities' resilience to cyber incidents[77] and whether they follow international guidance and industry best practices.[78] Deficiencies identified

[74] Consideration should be given to how these measures could take into account the interdependencies between big techs.

[75] As one example of regulatory action, in October 2021 the US Bureau of financial consumer protection ordered six big techs (Google, Apple, Facebook, Amazon, Square and PayPal) offering payment services to turn over information about how they exploit their payment platforms. See US Bureau of financial consumer protection (2021).

[76] See also BCBS (2022).

[77] As set forth in the BCBS Principles for Operational Resilience, a key component of banks' operational resilience (that is, a bank's ability to deliver critical operations through a disruption) is resilience to cyber incidents, including those that may arise from outsourcing arrangements.

[78] There are now various tools and frameworks available to help financial institutions improve their cyber security capabilities. These include the National Institute of Standards and Technology (NIST) Cybersecurity Framework, standards issued by the International Organization for Standardization (ISO) such as ISO-2700x, and guidance provided by the G7 Cyber Expert Group (ie *G7 Fundamental Elements of Cybersecurity for the Financial Sector*, issued in October 2016, and the *G7 Fundamental Elements for Effective Assessment of Cybersecurity*, issued in October 2017) and guidance from the FSB, which developed, inter alia, a toolkit of effective practices that aims to assist organisations in their cyber incident response and recovery activities.

in this assessment could be addressed with existing regulatory instruments (Table 5).[79] All this could be complemented by an assessment of authorities' own work in terms of full, timely and consistent implementation of relevant international standards such as the BCBS Principles for Operational Resilience and revised Principles for the Sound Management of Operational Risk.[80]

- **For regulated entities' use of critical services, authorities may wish to ramp up their monitoring efforts.** Enhanced monitoring should aim to identify risks that arise from regulated entities' increasing dependence on critical third-party service providers, including concentration and contagion risks and, at the macro level, systemic risks. The aim of this exercise, which could be undertaken through – or in concert with – industry-wide business continuity plan (BCP) testing, should be to reach a view of how financial institutions are connected through the services provided by global big techs, not only within the financial sector but also with relevant non-financial entities. A major concern in this respect is that the limited number of providers of cloud services could magnify the impact of any operational vulnerability.[81]

54. **In addition, some jurisdictions are taking action to implement direct oversight powers over providers of critical services.** In the EU, the proposed Digital Operational Resilience Act (DORA) will establish a framework on digital operational resilience in the financial sector. It will impose requirements on the security of network and information systems for a wide range of different entities involved in the provision of financial services; and introduce EU-level oversight of service providers that are critical for the financial system.[82] In the US, federal banking agencies already have oversight powers to monitor significant third-party service providers to banks (Crisanto et al (2021b)). Such powers, where available, could be used to ensure an adequate quality of operational risk management of critical service providers, and thereby indirectly strengthen the operational resilience of regulated institutions.[83]

[79] Financial authorities' approach to outsourcing and third-party relationships typically puts the onus on firms to ensure these relationships do not prevent them from complying with regulatory requirements.

[80] Relevant publications issued by the FSB include a report on existing approaches to cyber incident reporting that outlines ideas on how more harmonisation can be achieved.

[81] See FSB (2022).

[82] Brits et al (2021) differentiate between oversight under DORA and traditional supervision because DORA does not have any preconditions governing market entry and only a limited range of enforcement and sanction tools (eg follow-up recommendations after audits are not binding).

[83] Ideally, big techs establish policies for operational resilience at the group level to account for interdependencies. Where such an option is not provided under regulatory frameworks, requirements could also be placed at the level of the legal big tech entity that performs critical services.

Indirect approach: available regulatory instruments for banks — Table 5

| | |
|---|---|
| **Risk transmission through intragroup dependencies** | |
| ICT and operational interdependencies | - Principles for operational resilience and risk***<br>- Cyber resilience standards and guidelines[%]<br>- Outsourcing requirements<br>Capital requirements for operational risk |
| Reputational interdependencies | - Step-in risk management and measurement* |
| Financial interdependencies | - Prudential capital requirements<br>- Rules on related party transactions<br>- Limits on large exposures**<br>- AML/CFT requirements |
| **Risk transmission through external interconnections** | |
| Dependency of financial sector on big techs as critical service provider (eg cloud computing) | - Principles for operational resilience and risk***<br>- Cyber resilience standards and guidelines[%]<br>- Outsourcing requirements |
| Strategic alliances and partnerships<br>- Principal agent problem and potentially misaligned incentives<br>- Consumer protection issues: diffusion of accountability | - Capital requirements for credit risk, including securitisation<br>- Market conduct rules to protect consumers from unfair practices<br>- Disclosure requirements |

* See www.bis.org/fsi/fsisummaries/step-in_risk.pdf.

** See www.bis.org/fsi/fsisummaries/largeexpos.pdf.

*** The operational resilience principles focus on governance, operational risk management, business continuity planning and testing, mapping interconnections and interdependencies, third-party dependency management, incident management and resilient cyber security and ICT. See www.bis.org/press/p210331a.htm.

[%] See www.bis.org/bcbs/publ/d454.pdf.

Source: FSI.

## Section 6 – Concluding remarks

55. **Despite their diversity, big tech business models share a number of common features**. Big techs generally complement their core activities (eg e-commerce, social media, search engine) with a range of additional services, in particular financial and technology ones. These services are usually integrated in the digital platforms by "ecosystem binders" (ie applications and tools that facilitate and promote the use of the entire ecosystem such as super apps and loyalty schemes). In addition, big techs rely on client data to enhance their activities and make the ecosystem more attractive for its users. They are also continuously seeking to expand their operations, with big techs operating on either a regional or a global level. Finally, big techs benefit from intragroup and external dependencies.

56. **Strong intragroup dependencies among big tech entities call for risk assessment at the group level.** Big tech platforms are powered by multiple financial and non-financial separate legal entities. While legally separate, these entities rely on common payment systems to facilitate transactions across the entire ecosystem. In addition, they use the same technological infrastructure, computer applications and analytical tools to process information relevant for the group. They also rely on a common credit risk assessment system to evaluate clients and share customer data to make the ecosystem work. As a result of these interdependencies, an operational failure in one part of the big tech ecosystem may affect the operations of the entire group, which may have a reputational and financial impact on the provision of

financial services. As such, risks arising from big tech activities should not be assessed on a solo but at a group level.

57. **The activities of big techs and financial institutions are increasingly intertwined**. Both offer financial products and services through a variety of partnerships, including: (i) strategic alliances to facilitate payments in the big tech ecosystem; (ii) white labelling arrangements through which big techs perform customer interface functions of products and services of partner financial institutions; (iii) BaaS partnerships that allow big techs to integrate financial products and services from different providers into a single platform; (iv) big techs' use of their credit scoring systems to assess the eligibility of customers for certain services provided by partner financial institutions; and (v) arrangements to originate and/or distribute lending and insurance products.

58. **Enhanced transparency regarding big tech-financial institution partnerships would improve regulators' understanding of the risks involved.** Currently, it is unclear whether these arrangements provide incentives to increase risk-taking through, for instance, riskier lending. Additional transparency would facilitate understanding of the extent to which these arrangements create a wider surface for cyber attacks and other criminal activities. Moreover, from the consumer point of view, additional transparency would help to clearly identify responsibilities in case of failures to protect consumers. More generally, a comprehensive assessment of the risks involved in this type of partnership is particularly important since weaknesses or failures in the operations of a big tech could negatively impact the reputation of its partner financial institution.

59. **Financial institutions heavily rely on technology services provided by big techs, and this is likely to increase going forward**. This is particularly the case with respect to cloud computing and data analytics. Most financial institutions already use some form of cloud services or plan to switch to the cloud shortly. The provision of these services is highly concentrated, with only a few big techs dominating the market. Moreover, to protect or increase their market share big techs are making large investments in cutting-edge technology driven by their emphasis on privacy and security and on taking advantage of emerging technologies such as quantum computing. As a result of this and the comparatively lower investments by top financial institutions in emerging technology, the financial system's dependence on a few critical service providers is likely to increase going forward.

60. **Financial institutions' and regional big techs' dependence on global big techs' technology exacerbate systemic vulnerabilities**. The analysis in this paper confirms that both financial institutions and regional big techs rely on technological infrastructure and analytical tools developed by global big techs. This dependence on a small number of critical technological providers exacerbates operational and concentration risks that may arise if these providers were to experience significant disruptions.[84] These disruptions may be amplified by regional big techs and could have a broader impact on the global economy, in particular by affecting small and medium-sized enterprises and retail customers across jurisdictions.

61. **The existing regulatory framework was not formulated with closely connected digital platform ecosystems in mind, and hence misses the risks arising from interdependencies.** Big techs' operations in financial services are regulated based on sectoral regulatory regimes. As such, big techs are treated like any other company, and their regulatory treatment depends on the type of financial activities in which they are engaged. Yet regulatory instruments currently available under sectoral frameworks were not designed to mitigate the risks created by strong intragroup dependencies and external interconnections inherent in big tech business models, but rather to address traditional financial stability risks. It is therefore not surprising that sectoral laws and regulations have certain blind spots when applied to big tech groups and the new risks to financial stability they create.

[84] See also Furber (2020).

62. **Addressing interdependencies risks requires the development of specific entity-based rules for big tech operations in the financial sector.** These rules could take the form of a new regulatory framework that allows authorities to control risks emerging from the combination of financial and non-financial activities. As a foundation, this framework should follow an entity-based approach and impose requirements at the group level, including on strengthening operational resilience.

63. **In the short term, authorities can rely on an indirect approach to mitigate the financial stability risks posed by interdependencies.** There are a number of options available to them. One is to identify risks stemming from interdependencies for regulated financial entities that are members of big tech groups and evaluate potential risk mitigants. Another is to assess these entities' ability, and those of other regulated financial entities that partner with big techs or depend on their services, to withstand and mitigate disruptive events, including cyber attacks, and take measures to further strengthen operational resilience if needed. Yet another option for authorities is to ramp up their monitoring efforts in relation to critical third-party service providers and, depending on the regulatory framework, use direct oversight powers over them. In exploring these options, authorities can benefit from sharing information on their regulatory approaches and supervisory practices with each other.

# References


Alibaba Group Holding Limited (2020): "Fiscal Year 2020 Annual Report".

ANT Group (2020): "Hong Kong Initial Public Offering Prospectus", October.

Asensio, C, A Bouveret and A Harris (2022): "Financial stability risks from cloud outsourcing", *ESMA Working Paper*, no 2, May.

Bank for International Settlements (BIS) (2019): "Big tech in finance: opportunities and risks", *Annual Economic Report 2019*, June, Chapter III.

Basel Committee on Banking Supervision (2012a): *Core principles for effective banking supervision*, September.

——— (2012b): *Principles for the supervision of financial conglomerates*, September.

——— (2022): "Newsletter on third- and fourth-party risk management and concentration risk", March.

Berg, T, V Burg, A Gombović and M Puri (2018): "On the rise of FinTechs – credit scoring using digital footprints", *FDIC CFR Working Paper Series*, WP 2018-04, September.

Brits, H, G Cuijpers, N Jonker, M Lohuis, R Roerink, C ter Wal and A Zwemstra (2021): "Changing landscape, changing supervision: developments in the relationship between big techs and financial institutions", Netherlands Bank.

Carstens, A (2018): "Big tech in finance and new challenges for public policy", keynote address at the FT Banking Summit, 4 December.

Carstens, A, S Claessens, F Restoy and H S Shin (2021): "Regulating big techs in finance", *BIS Bulletin*, no 45, August.

CB Insights (2021): "The Big Tech In Quantum Report: How Google, Microsoft, Amazon, IBM, & Intel Are Battling For The Future Of Computing", December.

——— (2022): "The big tech in cybersecurity report: how Facebook, Apple, Microsoft, Google and Amazon are tackling cyber threats", January.

Chui, M (2021): "Money, technology and banking: what lessons can China teach the rest of the world?", *BIS Working Papers*, no 947, June.

Citi GPS (2018): "Bank of the future: The ABCs of digital disruption in finance", *Citi GPS: Global Perspectives & Solutions*, March.

Congressional Research Service (2022): "Big tech in financial services", May.

Crisanto, J C, J Ehrentraud and M Fabian (2021a): "Big techs in finance: regulatory approaches and policy options", *FSI Briefs*, no 12, March.

Crisanto, J C, J Ehrentraud, A Lawson and F Restoy (2021b): "Big tech regulation: what is going on?", *FSI Insights on policy implementation*, no 36, September.

Croxson, K, J Frost, L Gambacorta and T Valletti (2022): "Platform-based business models and financial inclusion", *BIS Working Papers*, no 986, January.

Danielsson, J and R Macrae (2019): "Systemic consequences of outsourcing to the cloud", VoxEU.org, 2 December.

Dierick, F (2004): "The supervision of mixed financial services groups in Europe", *ECB Occasional Paper,* no 20, August.

Ehrentraud, J, J Prenio, C Boar, M Janfils and A Lawson (2021): "Fintech and payments: regulating digital payments services and e-money", *FSI Insights on policy implementation*, no 33, July.

Ehrentraud, J, J Evans, A Monteil and F Restoy (forthcoming): "Big tech regulation: in search of a new framework", *FSI Occasional Papers*.

Feyen, E, J Frost, L Gambarcota, H Natarajan and M Saal (2021): "Fintech and the digital transformation of financial services: implications for market structure and public policy", *BIS Papers*, no 117, July.

Financial Stability Board (FSB) (2019a): *BigTech in finance: market developments and potential financial stability implications*, December.

——— (2019b): *Third-party dependencies in cloud services. Considerations on financial stability implications*, December.

——— (2022): *FinTech and Market Structure in the Covid 19 Pandemic Implications for financial stability*, March.

Financial Time (2022): "Apple sidelines Goldman Sachs and goes in-house for lending service", June.

Fortune Business Insights (2021): "Cloud computing market – market research report", October.

Frost, J, L Gambacorta , Y Huang, H S Shin and P Zbinden (2019): "Big tech and the changing structure of financial intermediation", *Economic Policy*, vol 34, no 100.

Furber, S (2020): "As 'big tech' dominates cloud use for banks, regulators may need to get tougher", 18 August.

Gartner (2021a): "Gartner Says Four Trends Are Shaping the Future of Public Cloud", August.

——— (2021b): "Gartner Says By 2023, 65% of the World's Population Will Have Its Personal Data Covered Under Modern Privacy Regulations", September.

Google Cloud (2021): "The financial services industry sees increasing public cloud adoption as driving innovation and compliance", July.

Gruson, M (2005): "Supervision of financial conglomerates in the European Union", Chapter 13 "Current developments in monetary and financial law, volume 4, IMF.

International Banking Federation (IBF) and O Wyman (2020): *Big banks, bigger techs? How policymakers could respond to a probable discontinuity*, July.

International Monetary Fund (2022): "BigTech in financial services: regulatory approaches and architecture", Note 2022/002, January.

Jenkins, J (2011): "How Amazon.com migrates to AWS", *2011 AWS Tour Australia*, closing keynote, July.

Khan, L (2021): "Comment Submission of Chair Lina M. Khan on the CFPB's Inquiry Into Big Tech Payment Platforms", December.

Klein, A (2019): "Is China's new payment system the future?", Brookings Institution, June.

Prenio, J, and J Yong (2021): "Humans keeping AI in check – emerging regulatory expectations in the financial sector", *FSI Insights on policy implementation*, no 35, August.

Rakuten Today (2019): "Rakuten's Alris marketing agent is finding customers that brands didn't know existed", March.

Rakuten (2020): "Annual report fiscal year 2020".

——— (2021): "Q2 FY2021 Financial Results Highlights", August.

Restoy, F (2019): "Regulating fintech: what is going on and where are the challenges?", speech at the ASBA-BID-FELABAN XVI Banking public-private sector regional policy dialogue on "Challenges and opportunities in the new financial ecosystem", Washington DC, 16 October.

——— (2021): "Fintech regulation: how to achieve a level playing field", *FSI Occasional Papers*, no 17, February.

——— (2022): "The digital disruption: The role of regulation", speech at the virtual conference by the Asia School of Business and the BIS, January.

Ruane, J, A McAfee and W D Oliver (2022): "Quantum computing for business leaders", *Harvard Business Review*, January–February.

Strauss, I, T O'Reilly, M Mazzucato and J Ryan-Collins (2021): "Crouching tiger, hidden dragons: how 10-K disclosure rules help Big Tech conceal market power and expand platform dominance", UCL Institute for Innovation and Public Purpose, *IIPP Policy Report* no 2021/04, December.

Synergy Research Group (2022): "As Quarterly Cloud Spending Jumps to Over $50B, Microsoft Looms Larger in Amazon's Rear Mirror", February.

The Economist (2020): "Do Alipay and Tenpay misuse their market power?", August.

The Washington Post (2021a): "How Big Tech got so big: Hundreds of acquisitions", April.

——— (2021b): "Amazon Web Services experiences another big outage", December.

US Bureau of consumer financial protection (2021): "Notice and Request for Comment Regarding the CFPB's Inquiry into Big Tech Payment Platforms", October.

Van der Spek, L and S Phijffer (2020): "Will bigtechs change the European payments market forever?", *Compact*, 2020/2, "Payments & Business Technology".

Zamil, R and A Lawson (2022): "Gatekeeping the gatekeepers: when big techs and fintechs own banks – benefits, risks and policy options", *FSI Insights on policy implementation*, no 39, January.