

Big tech interdependencies – a key policy blind spot¹

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.