BBVA Comments to BCBS Sound Practices Paper: Implications of fintech developments for banks and bank supervisors

October 31, 2017

BBVA

General remarks

BBVA appreciates the opportunity to comment on the Basel Committee on Banking Supervision's (BCBS) consultation on the implications of fintech for the financial sector. We value the Committee's assessment of the benefits and risks arising from financial innovation and we are grateful to global standard-setting bodies such as the BCBS for the ongoing work in this area. While we agree with the BCBS' observations and recommendations in general terms, we believe that certain areas would benefit from further consideration or greater clarity.

BBVA is keen to continue supporting the BCBS in this endeavour, and we are looking forward to discussing any of the issues covered in this paper with the authorities in order to contribute to a strong and safe financial sector. The following is a non-exhaustive list of BBVA's previous research on this field, as well as our contributions to past public consultations from authorities and institutions at the EU and international level.

- Latest issue of BBVA Research Digital Economy Outlook (quarterly publication)
- González-Páramo, J.M. (2017) Financial Innovation in the Digital Age: Challenges for Regulation and Supervision. Revista de Estabilidad Financiera nº32. Banco de España.
- Sebastián, J. (2017) Blockchain in financial services: Regulatory landscape and future challenges for its commercial application. BBVA Research Working Paper
- Cerqueira, O.; Dos Santos, E.; Fernández de Lis, S.; Neut, A.; Sebastián, J. (2017) Central Bank Digital Currencies: assessing implementation possibilities and impacts. BBVA Research Working Paper
- BBVA Response to the European Commission's public consultation document on FinTech (*FinTech: a more competitive and innovative European financial sector*). June 2017
- BBVA Response to the European Banking Authority's Consultation on reccomendations on outsourcing to cloud service providers

Broadly speaking, **we believe there are three main areas where a deep reflection on the part of the BCBS, bank supervisors and regulators and the financial industry is essential: (1) the concept and categorisation of the fintech phenomenon, (2) the understanding of what is behind a true level playing field and (3) the increased role of data as a driver of change in the structure and functioning of the financial sector.** We will now discuss each of these three issues in turn. This will be followed by specific comments to the scenarios and the observations and recommendations.

1. The concept and categorisation of the fintech phenomenon

The BCBS has decided to use the FSB's definition of Fintech[1], which is inclusive. We completely support this definition, as it is consistent with the vision of the financial services market as a fast-evolving ecosystem that includes banks, new entrants, BigTech companies and also regulators. It is clear from the FSB's Fintech definition that the key to define fintech is the innovative application of exponential technologies to revamp the provision of financial services, regardless of the nature and size of the provider of the services.

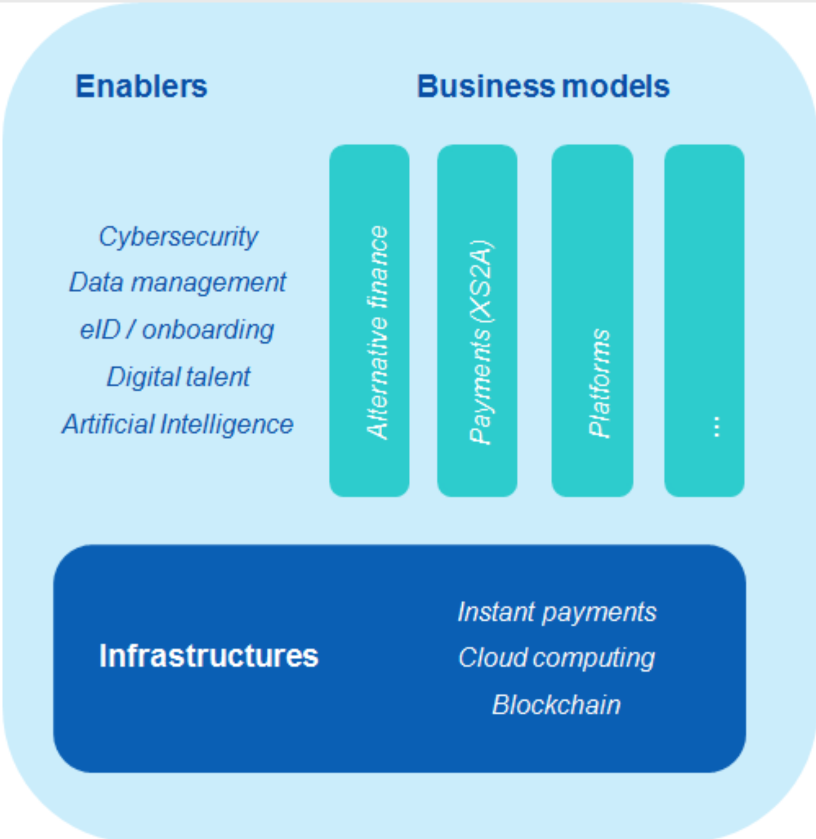
However, in the description of the fintech landscape that builds on the results of the survey, the BCBS seems to identify fintech firms with smaller new entrants, without encompassing banks or big technological companies. This seems inconsistent with the definition of fintech and may result in an overestimation of the short-term impact of start-

[1] The FSB defines Fintech as "technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services".

ups and an underestimation of that of BigTech companies. We agree with the BCBS's view that the definition can influence how supervisors approach fintech, and therefore suggest to ensure that the term is used consistently throughout the document.

Regarding the categorisation of fintech innovations, in BBVA has developed a simple analytical framework that differentiates innovations from the perspective of digital regulation. Our framework considers three broad digital domains in which regulation will play a role in shaping the future of digital financial services: digital enablers, infrastructure and vertical innovations in the form of new business models (see Figure 1).

Figure 1



Source: BBVA

The *digital enablers* refer to some relevant issues which affect potentially almost any digital financial service, and therefore require an enabling regulatory framework. This includes topics like cybersecurity, data protection, digital identity, artificial intelligence and the ability of financial service providers' to attract and retain the best digital talent.

The *digital infrastructure* refers to emerging technologies that have the potential to disrupt how the financial system infrastructure will work in the future. Any response from regulators should consider how the industry intends to leverage these technologies in order to provide effective regulations. This block includes technologies such as cloud computing, blockchain and payment infrastructures with real-time capabilities.

Finally, there is a number of vertical innovations that imply the emergence of *new business models*, activities or new ways of providing existing services. These rest on technological advances and changes in customer demands, and are sometimes driven by third-party access to bank accounts or financial data. Most of these innovations take the form of digital platforms that act as intermediaries in two-sided markets (e.g. between providers of goods and services and end-consumers). In the platform economy, markets reconfigure, and consumers interact with both the providers of products and services and with the platform itself. Therefore, they give rise to new consumer protection risks and competition concerns and may eventually, in the case of financial services platforms, have an impact on financial stability. Obviously, this demands a close monitoring from authorities, who should contemplate as well the possibility that banks become back-end providers of services (through APIs), financial services platforms or both.

When assessing the impact of new technologies on the banking industry, an additional factor should be considered. The irruption of technologies that have achieved large-scale adoption in a short period of time has triggered a profound reshaping in the way of providing financial solutions. So-called exponential technologies, such as the internet, mobile, social media, cloud or big data analytics, are already mature and driving an exponential decline in costs. These technologies, and their interactions with others in more nascent stages (artificial intelligence, digital currencies or blockchain), constitute a differentiating factor that explains the speed of changes and that considerably broadens the field of opportunity to work in the benefit of consumers.

Therefore, beyond the possibility of fintech being hyped or not, it seems certain that changes to consumer behavior, technology and business are already reshaping the economy and the financial sector, and will further continue to do so in the future. As an illustration of this, the apparent decline in VC investments may be explained to a certain extent by a substitution effect with Initial Coin Offerings[2].

2. The understanding of what is behind a true level playing field

In our view, the principle of level playing field ought to comprise two aspects. **First, activities involving the same risks in terms of financial stability, consumer protection and the integrity of the financial system should receive the same regulatory treatment.** Therefore, any difference in regulation and supervision should be based on the risks posed by different products and services. **Second, there should not be unnecessary barriers to competition in the market beyond those justified by risk considerations.** This means, for example, granting different types of players access under fair conditions to payments infrastructure, customer data, and regulatory and supervisory guidance, where the latter is aimed at keeping unavoidable risk-justified regulatory barriers to a minimum.

Regarding the first aspect, there are two main sources of unlevelled playing between banks and non-bank players.

- **One arises from the regulatory framework currently applicable to banks.** Banking groups are subject to prudential regulations that have implications for most of their businesses, including those in which they compete with non-bank players that are only subject to activity-specific regulations or benefit from regulatory loopholes. Therefore, FinTech activities are generally subject to additional rules on internal governance when they are carried out within a banking group. Rules on remuneration (as in European regulation), internal governance and outsourcing requirements leave banks in a situation of competitive disadvantage in terms of cost, time-to-market and talent attraction and retention. Regulations on consumer protection and AML/CFT are generally activity-specific, and therefore more aligned with the principle of level playing field.

- **Existing loopholes in the regulatory framework are another source of an uneven playing field between banks and nonbank players.** Some new services or business models are not yet covered under existing regulations. In this regard, the results of a mapping exercise conducted by the European Banking Authority

---

[2] For instance, a report from the research firm Autonomous published in 2017 suggests that almost $1.3bn has been raised in the first half of 2017 by start-up technology companies via "initial coin offerings, an amount far higher than the volume of venture capital investment into Blockchain and Bitcoin firms.

(EBA) earlier this year are quite telling. The EBA has found that a significant proportion of fintech firms in the EU (31% of the sample[3]) are not subject to any regulatory regime at all. Furthermore, although the EBA identifies that there are over 1500 fintech companies in the EU, detailed information could only be obtained for 282 companies, suggesting that the number of unregulated firms could even be higher.

This means that not only are potential risks to financial stability, consumer protection and the integrity of the financial system left unaddressed, but also asymmetries between players arise, given that regulated providers often face obstacles to engaging in unregulated activities. A clear example of this is the European Banking Authority's opinion in 2014, which called on national supervisory authorities to prevent credit institutions, payment institutions and e-money institutions from buying, holding or selling virtual currencies.

The second aspect of the level playing field principle refers to the removal of unnecessary barriers to fair competition. The following issues have been identified in the European context, but are useful to illustrate the concept:

- **Asymmetry in the contribution to the payments infrastructure:** The new EU Payment Services Directive (PSD2) works towards the removal of unnecessary barriers to fair competition by allowing non-banks authorised as payment service providers to access bank account data and initiate payments on behalf of clients. However, since these third-parties will not pay for accessing bank accounts, this imposes an unfair burden on banks and creates an asymmetry in the contribution to the sustainability of the payments infrastructure.

- **Non-standardized access to personal data.** Asymmetries between players may arise due to sector regulations on third-party access to customer data (such as PSD2 in the EU and the Open Banking Standard in the UK) and the new General Data Protection Regulation (GDPR). Although the latter will bring in a new right to data portability which applies to all sectors, the way of accessing customer data will be less standardized than in PSD2 and will only affect individual customer data (whereas PSD2 also applies to business accounts).

To ensure a level playing field among all providers of financial services, be they banks or not, the regulatory and supervisory framework should progress on three fronts:

- **Limiting the implications of prudential regulation for non-core businesses (i.e. ringfenced, non deposit-taking activities) in which banks compete with non-bank players.** The internal governance of these businesses should be subject to the same activity-specific regulations that apply to non-bank players. To this end, either temporary exceptions within the regulatory framework or exclusions from the perimeter of prudential consolidation could be allowed.

- **Plugging existing gaps in the regulation by developing a regulatory and supervisory framework for new services,** such as virtual asset management, alternative finance or financial service marketplaces. **These rules should apply to both banks and non-bank players, the latter being authorised by narrowly defined (activity-specific) FinTech licenses.**

- **Facilitating innovation for all players, under safe and even conditions**, in case regulatory obstacles or uncertainties come to hinder the development of innovative solutions that would benefit consumers. **Regulatory sandboxes are a useful tool in this respect.** Our views on regulatory sandboxes are further developed under Recommendation 10.

[3] The sample refers to the subset of 282 on which the EBA has detailed information

3. The increased role of data as a driver of change in the structure and functioning of the financial sector

As outlined in the previous comment, data is an essential input in the provision of financial services. Due to the existence of information asymmetries between potential borrowers and lenders, having access to appropriate, high-quality data is particularly relevant for credit granting. However, the importance of data is by no means limited to credit provision. Rather, it is essential also for providing financial advice and other value-added services.

At a time in which digitalisation is making storing, processing and sharing large amounts of data technically feasible, open banking regulations in some jurisdictions (the aforementioned PSD2 and GDPR in the EU or the Open Banking Standard in the UK) introduce a right to data portability that allows customers to share their data with third parties. In this context, obtaining the customers' trust is the cornerstone for success. In fact, trust and access to customers' data interact in a virtuous circle that can be characterized as follows. Clients' trust is key to obtaining their consent to access their data. The more data institutions have, the more insight they will be able to build on their clients, and therefore the more personalized and appreciated value-added services they can create for them. Enhanced customer experience will contribute to reinforce client satisfaction and trust on the organisation.

Consistent with scenarios 3 and 4 in the BCBS Sound Practices paper, greater accessibility to customer data by third parties will most likely lead to increased competition among the final providers of financial products and services, as well as to introduce relevant changes in the distribution of financial services by disintermediating the relationship between customers and providers. In fact, nowadays, a number of new intermediaries offer account-information services, comparison tools, personal financial management (PFM) services or different marketplaces in which customers can directly sign up for different financial products (i.e. deposits).

As we will detail in our comments to the scenarios, this trend can be seen as a first step towards the development of broad financial services platforms, which act as intermediaries between end-customers and different providers of financial services (banks, specialized firms, etc.) in a two-sided market. Several trends emerge in this new environment, which will likely result in a reconfiguration of the structure of the financial services market. On one hand, this scenario facilitates the comparability of products and services and lowers the cost of switching between providers, thus leading to increased competition among providers. In this context, it would be reasonable to expect more concentration in the more standardized activities and products, but a more fragmented market for the more specialized ones. On the other hand, digital platforms tend towards market concentration on a reduced number of players due to both network effects and economies of scale. This reconfiguration of the market structure will change the distribution of risks across the financial services ecosystem, thus calling for a regulatory framework that clearly allocates the liabilities across the different players. Moreover, ensuring a level playing in the access to data, in which regulatory obligations towards openness are symmetrical between sectors and fair for players bearing the underlying infrastructure and data enhancement costs, becomes more important than ever.

The forward-looking scenarios

1. Better bank scenario

In line with this scenario, many banks are already taking action to survive and thrive by attempting to make use of new innovations to create new value propositions for their clients. In this process, banks face some competitive disadvantages in comparison with other digital competitors (including big internet players and smaller new entrants), with more flexible business models and without outdated legacy structures.

Banks, therefore, need to embark in a profound transformation process that demands overcoming several internal barriers, including modernising their IT infrastructures and, most critically, an evolution of talent and culture within the organisation. These are profound changes that require a reinvention of the business and the organisation and significant investments. Two forces are essential to achieve this transformation. The first is internal in nature, and refers to the banks' capacity for self-transformation. The second, is the role of the regulation as an obstacle or driver.

In this sense, as already commented in our second remark in the General remarks section, regulation and supervision play an essential part in explaining some of the main asymmetries between bank and non-bank players. As a result, fintech activities are usually subject to more stringent regulation when they are performed within a banking group than if they are provided by other types of institutions. Rules on remuneration (as in European regulation), internal governance and outsourcing requirements leave banks in a situation of competitive disadvantage in terms of cost, time-to-market and talent attraction and retention.

2. New bank scenario

We see this scenario as less likely to materialize. Although it is true that, compared to incumbents, neobanks benefit from greater agility and efficiency due to the absence of legacy infrastructures and physical distribution networks, they face practically the same regulatory restrictions. Furthermore, they face the difficulty of gaining customer trust from scratch, which may demand them to differentiate their products considerably from existing offerings. Finally, once their clients become more sophisticated, they may not be able to satisfy all of their financial needs as these banks usually offer a limited product spectrum. However, we believe there is room for this type of players in a richer and more complex financial services ecosystem.

3. Distributed bank

This scenario may present some limitations due to difficulties banks face in forging the type of alliances described. Regulatory requirements may explain some of these difficulties, such as those related to the control of operational risk in outsourcing or restrictions arising from data protection rules. On the contrary, the trend towards APIfication of financial services and Banking as a Service (Baas) as well as regulatory initiatives such as the revised European Payment Services Directive (PSD2) and the Open Banking Standard (OBS) in the UK might trigger dynamics towards this scenario. In particular, PSD2 grants access to bank accounts to third-party providers (TPPs), acting on behalf of the client, while the OBS in the UK goes a step further in facilitating the functioning of platforms by requiring the largest retail banks to develop and maintain open API standards to release open data for financial products (e.g. product information, terms and conditions), which would facilitate advisory roles from a technical and regulatory standpoint.

Also, the new General Data Protection Regulation (GDPR) works towards this scenario, as it introduces a right to data portability that will allow firms to have access to customers' data in the hands of other companies. However, firms are only "encouraged" to develop interoperable formats and data will only have to be directly transmitted between firms "where technically feasible". In contrast, under PSD2, transactional data from bank accounts will have to be directly transmitted between banks and TPPs and subject to certain standardization. As commented in the General remarks section, this will create an unlevelled playing field in the access to data that favours those players that already have access to large amounts of data. Besides, digital markets with platforms business models tend towards concentration, which may generate a dynamic that makes this scenario not stable in time and conducive to a highly concentrated market, dominated by large digital platforms as depicted in scenario #4.

4. Relegated bank

The world depicted by this scenario is dominated by digital platforms. This innovation is already pervasive in many other sectors, where some successful business built on this model have achieved an immense scale (Amazon, Uber, Airbnb…). In the financial sector, this model is still in an earlier stage (e.g. vertical-specific marketplaces, comparison sites, etc.) but this trend is expected to continue gaining momentum, as it has happened in other informational sectors.

Digital platforms have the capacity to reconfigure the financial services sector as they have done in other sectors, and usually markets in which digital platforms dominate tend towards concentration. Consequently, these may give rise to new risks in terms of customers' lock-in or anti-competitive practices (due to the large bargaining power associated with the scale of these platforms). Furthermore, it may even have a negative impact on financial stability by an increase in systemic risk driven by the need to achieve a larger scale in a commoditised business. Hence, in this scenario authorities would have to closely monitor the emergence of new business models to ensure the regulatory framework guarantees consumer protection, financial stability and fair competition.

5. Disintermediated bank

Together with the "New bank" scenario (#2), this fifth scenario seems the most unlikely. First, because it would be hard to find a sufficient number of providers that generate enough trust among customers to centralize the offering of niche products. Furthermore, in the absence of providers able to bring a client the full range of products desired (one stop shop model), it seems unlikely to expect customers will be willing to assume the cost in terms of money and time of comparing among and dealing with many different providers to manage their finance.

Observations and Recommendations

Table 1. Summary of BBVA's Comments to the BCBS' Observations and Recommendations

Recommendation	Summary of BBVA's Comments
1. Balance between ensuring safety and promoting innovation	Developments in technology and new market dynamics generate new risks, or change the nature and scope of existing ones, and challenge the fulfillment of the four traditional objectives of financial regulation (financial stability, financial integrity, consumer protection and enhanced efficiency and competition of the system). The identification and understanding of these new risks is a must, prior to the design of any regulatory framework, to ensure that it is holistic and future-proof, and conducive to a level playing field in the financial sector.
2. Effective structures for governance and risk management	Policies on management processes and internal governance should be applied proportionally. A risk-based approach that takes into account specific activity risks, and not whole company risks by default is needed. Otherwise, smaller players would be better suited for disruption, creating less chances for incumbents to transform themselves, thus creating greater financial instability
3. Implications of using enabling technologies	The level of maturity and understanding of these enabling technologies differs considerably. In the case of cloud, the rate of adoption of this technology in the banking sector is significantly slower than in other sectors, driven by the complexity of banking IT systems, but also to reluctances from financial supervisors and regulators. However, as new entrants that construct themselves on this technology continue to gain market share, an excessively conservative approach might make it very difficult to maintain the competitiveness of the sector.
4. Implications of the use of third parties (outsourcing and/or partnerships)	There are several regulatory and supervisory obstacles that hinder the opportunities of banks to partner and/or outsource to third parties. Furthermore, banks are subject to stricter requirements in terms of internal policies and notification/authorization from supervisors than other players, such as bigtech companies, when partnering with fintech companies, and this contributes to an unleveled playing field.
5. Cross-sectoral cooperation between supervisors and other relevant authorities 6.International cooperation between banking supervisors	This is essential to achieve a true level playing field in the financial sector. Cooperation and collaboration among regulatory authorities is needed across sectors (including non-financial regulators such as data protection authorities, consumer protection authorities, and other digital-related bodies) and across jurisdictions. It is essential to establish a continuous and open dialogue that incorporates the private sector.

7.Adaption of supervisory skillset	Regulators and supervisors need to invest in new skills to allow them to understand and manage new technologies, businesses and risks. This can be achieved through training of staff and a targeted recruitment policy. Regarding the latter bank supervisors may encounter severe difficulties for attracting and retaining staff. This is a problem also for banks, who face hurdles arising from some prudential regulations on top of that.
8. Opportunities for supervisors to use innovative technologies (suptech)	The development of regtech and suptech solutions can provide benefits to the whole financial services industry and to the authorities, as it eases the relationship among them and facilitates the process of reporting and monitoring.
9. Relevance of existing regulatory frameworks	We support the need to review the existing regulatory, supervisory and licensing frameworks. To this end, we support the implementation of certain narrow fintech licences for specific activities, as long as the level playing field is ensured. These licences should be activity and risk specific and should not be understood as a shortcut to provide additional services outside the scope of the initial license. Banks should be allowed to conduct any activity subject to narrower fintech licenses.
10. Regulatory initiatives to facilitate innovation	Regulatory sandboxes, if adequately implemented, offer promising benefits for regulators, consumers, fintech startups and incumbent banks alike. Regulatory sandboxes should be ruled by clear ex-ante principles to ensure fairness and avoid arbitrariness, although flexibility is also needed to quickly address the specificities that are inherent to any innovation. To ensure a level playing field between new players and established firms, participation in the sandbox should be voluntary and open to all parties. Different regulatory and supervisory bodies (prudential, consumer protection, data protection, AML/CFT, etc.) should be involved.

Source: BBVA

BCBS Recommendation 1: *Banks and bank supervisors should consider how they balance ensuring the safety and soundness of the banking system with minimising the risk of inadvertently inhibiting beneficial innovation in the financial sector. Such a balanced approach would promote the safety and soundness of banks, financial stability, consumer protection and compliance with applicable laws and regulations, including anti-money laundering and countering financing of terrorism (AML/CFT) regulations, without unnecessarily hampering beneficial innovations in financial services, including those aimed at financial inclusion.*

BCBS Recommendation 2: *Banks should ensure that they have effective governance structures and risk management processes in order to identify, manage and monitor risks associated with the use of enabling technologies and the emergence of new business models and entrants into the banking system brought about by fintech developments. These structures and processes should include:*

- *robust strategic and business planning processes that allow banks to adapt revenue and sound new product approval and change management processes to appropriately address changes not only in technology, but also in business processes;*
- *implementation of the Basel Committee's Principles for sound management of operational risk (PSMOR) with due consideration to fintech developments;*
- *monitoring and reviewing of compliance with applicable regulatory requirements, including those related to consumer protection, data protection and AML/CFT when introducing new products, services or channels.*

BBVA Comments on Recommendation 2:

We broadly agree with recommendations 1 and 2. The digital disruption may be beneficial for the financial sector in facing the environment of low growth, reduced profitability, high regulatory pressure and damaged reputation. However, developments in technology and new market dynamics challenge the fulfillment of the four traditional objectives of financial regulation, namely: (i) financial stability, (ii) financial integrity, (iii) consumer protection and (iv) enhanced efficiency and competition of the system. The digitalization of financial services generates new risks, or may change the nature and reach of existing ones, which are not fully covered by traditional regulatory and supervisory approaches, and that have implications on each of the aforementioned objectives.

The identification and understanding of these new risks is therefore a must prior to the design of a regulatory framework that ensures the safety and soundness of the system without hindering innovation. Only with this understanding would it be possible to achieve a regulatory approach that is **holistic**, combining financial and non-financial regulations such as data protection, cybersecurity, etc.; and **future-proof**, which means being flexible enough not to become outdated by rapidly evolving technologies and a dynamic business ecosystem. And, what is more, this is essential to achieve a **level playing field** in the financial sector as the one described in the General Remarks section.

A **recent paper** written by **Dr. González-Páramo**, BBVA Executive Board Member, in Banco de España's Financial Stability Review[4] presents a thorough analysis of the potential benefits of the digitisation of finance and of the new risks (in terms of stability and integrity of the financial system, and consumer protection) that digital infrastructures, business and distribution models and customer solutions may pose, and the expected regulatory and supervisory response. We believe that this could be of interest for the BCBS' analysis and future work.

The paper presents **an analytical framework that first summarizes the main changes and disruptions** that are taking place in three blocks **(infrastructure, banking products and distribution)** and then assesses the impact of those changes. For the latter, the paper first presents **the potential efficiency gains, and then the implications,** which may be positive, negative or ambiguous, **for financial stability, financial integrity and the protection of financial consumers.**

Adding to the analysis presented by the BCBS behind observations 1 and 2, this paper contains valuable insights that we summarize below:

On the risks:

- When assessing the **impact on financial stability**, increased competition could also have negative consequences (different from the positive impact identified by the BCBS). In fact, increased competition could add pressure on the profitability of financial institutions, by lowering margins and threatening the existing cross-selling and cross-subsidy strategies. Furthermore, the impact of intermediation services on the concentration of risks seems more complex than outlined by the BCBS. In fact, more intense competition could lead to market concentration on a reduced number of players that would be able to benefit from large economies of scale. This effect is likely to be prevalent for highly commoditisable products, and might lead to increased concentration in financial stability risks.

[4] José Manuel González-Páramo. Financial innovation in the digital age: Challenges for regulation and supervision. Banco de España, Financial Stability Review Num. 32. May 2017

- Another impact on financial stability is the possible emergence of **new single point of failure risk** if there is a **concentration in the providers of cloud services** for the banking sector. This is likely to happen considering (i) the economies of scale in the provision of cloud computing services, and (ii) the specific and more stringent requirements for providing these services to the financial industry, which lead to financial service providers relying in big technological companies such as AWS, Microsoft or Google.

- Regarding **liquidity risk and the volatility of bank funding sources**, there is an additional risk worth mentioning. The combination of real-time payment systems with advice and automation tools might further contribute to increase the volatility of deposits, exacerbating liquidity risks and the possibility of bank runs.

- On the increase of **conduct risks** of banks associated with the **allocation of responsibilities** when services are offered by different providers, it is worth noting that the situation described in the Sound Practices paper might lead to an unleveled playing field among providers. This is the case, for instance, of marketplaces in which consumers can directly sign up to products from different providers. In this context, the lack of a regulatory framework generates uncertainty as regards the allocation of liabilities, and whether the responsibility lies with the provider or the platform. As platforms are not regulated, this would ultimately lead to an overburden of the liability on the providers. However, in the case of outsourcing risk, this ambiguity must be solved in the contracts signed between the outsourcing institution and the provider, as well as in Service Level Agreements (SLA).

- Finally, **cyber security** risks have become a growing concern among authorities, who are especially worried due to the increased digitization of financial services. However, cybersecurity depends on a lot of factors, and it is not only relevant in this new digitized environment. In fact, in some cases legacy IT infrastructures may be even more vulnerable to cyber attacks than newer, more innovative solutions. Still, given the huge economic damage that cyber threats may create, as well as an overall lack of confidence on the part of authorities in the safety and security of digital technologies, innovation may end up being constrained. In this sense, the use of international recognized standards on cybersecurity would help to create at least a minimum baseline for all players in the industry. A new certification or labelling system should be created, following a principle-based approach, and incentivised. Furthermore, regulators should seek to simplify the current regulatory framework, creating a one-stop-shop mechanism for incident reporting regardless of the regulation setting the obligation and harmonizing incident reports and taxonomies. Finally, regulators should promote information sharing about attempted or actual cyber-incidents, being as proactive and efficient as possible.

On the opportunities:

- Regarding **regtech**, as outlined by the BCBS, it allows to automate and enhance tasks that require a comprehensive understanding of regulation and compliance, such as AML, financial reporting or risk management. Thus, the development of RegTech solutions can provide benefits to the whole financial services sector as well as to authorities, as it will easen the relationship among these parts. On this topic, recent work by the Institute of International Finance (IIF)[5] provides highly valuable insights, by identifying main bottlenecks in compliance and regulatory reporting that could benefit from regtech, and discussing barriers to regtech implementation and development of the regtech market. Also, the IIF is currently exploring the use of machine learning for AML and risk modelling.

- Solutions like shared KYC utilities could be highly useful to facilitate compliance with KYC/due diligence requirements under AML/CFT rules. However, since banks are still liable for information retrieved from third parties, they still need to double-check any information obtained from a shared KYC utility. For shared utilities

[5] See IIF (2016), *RegTech in Financial Services: Technology Solutions for Compliance and Reporting*

to really add value, banks should be assured when they can employ this information as a substitute, and not only as an input, of their own CDD procedures. Furthermore, access to public registries should also be allowed, as it would facilitate compliance with AML/CFT rules.

Finally, in relation to Recommendation 2, and the need to ensure sound product approval and compliance with regulatory requirements when introducing new products, services or channels, we would like to stress the importance of proportionality. A risk-based approach that takes into account specific activity risks, and not whole company risks by default is needed. Otherwise, smaller players would be better suited for disruption, creating less chances for incumbents to transform themselves, thus creating greater financial instability. In this sense, we should bear in mind that key performance indicators (KPIs) used to measure traction (or success) of digital transformation initiatives will not necessarily impact revenue streams in the short term.

BCBS Recommendation 3: *Banks should ensure they have effective IT and other risk management processes that address the risks of the new technologies and implement the effective control environments needed to properly support key innovations*

BBVA Comments on Recommendation 3:

Big data analytics and artificial intelligence are technologies with a great potential to further expand the access to financial services by lowering the complexity and the costs associated with certain advisory and credit scoring services. Furthermore, technologies such as cloud computing or distributed ledger technologies (DLT) address cost inefficiencies at the core of the banking infrastructure. Specifically, cloud computing allows for greater scalability, flexibility and reduced time-to-market. Also, cloud computing explains the recent APIfication trend, and is behind the digital platforms model.

When assessing these enabling technologies, however, it is important to bear in mind that the level of maturity of these innovations, and therefore the depth in the understanding of the risks associated, differs considerably. In the case of cloud, the rate of adoption of this technology in the banking sector is significantly slower than in other sectors, driven in part by reluctances from financial supervisors and regulators, and oftentimes, banks. However, as new entrants that construct themselves on this technology continue to gain market share, this excessively conservative approach might make it very difficult to maintain the competitiveness of the sector.

- Distributed ledger technology (DLT)

DLTs are still relatively immature technologies and, as such, are subject to diverse challenges in different fields. Moreover, some technological issues remain unsolved, as well as a lack of technical and operational standards. Some of the most relevant challenges in relation to DLTs include: scalability, interoperability, cybersecurity, privacy and security against money laundering and fraud. Also, some operational issues arise, including the management of the transition from current infrastructures to DLTs, the needed acquisition of DLT-related knowledge and skills by the corporate workforce involved in these projects, and the governance of DLs from the point of view of accountability and rules of participation of nodes in every DL network.

All in all, the immaturity of DLT and the piloting phase of identified use cases means that specific regulation of DLT activities in the financial services industry is still almost non-existent. Although some regulations in place will apply to DLT-based services, when looking at the big picture in DLT, there are a number of broad regulatory challenges that will have to be addressed at some point in the future[6]:

---

[6] For further reference and detail on this, please check BBVA Research's "Blockchain in financial services: Regulatory landscape and future challenges"

- Inclusion of payments and international transfers service providers using DLT in KYC, AML / CFT regulations in order to ensure a level playing field and control potential illicit uses of cryptocurrencies.
- Exchange platforms and custodian wallet providers were already proposed for inclusion in the 4th European AML Directive on July 2016.
- Legal framework regarding the nature of DLT, specially in terms of how to deal with territoriality and liability issues.
- Legal framework for the recognition of DL as single sources of truth.
- Regulation on how the “right to be forgotten” shall be interpreted to avoid collision with the immutability of the DL.
- Legal framework on the validity of documents stored in the DL as a proof of possession or existence.
- Legal framework on the validity of financial instruments issued on the DL.
- Legal framework on the issuance of crypto-tokens (namely Initial Coin Offerings or ICOs) clarifying if they must be treated as securities, crowdfunding schemes or other kind of instruments depending on the characteristics of that issuance and the purpose of the tokens.
- Legal framework for smart contracts in terms of territoriality, liability and real-world enforcement.
- Legal framework for information in DL from the perspective of cross-border flow of data and data protection.
- Legal framework regarding the use of DLT as a valid ruling register for the Internet of Things (IoT).
- Definition of regulatory reporting standards on DLT when using them as tools for compliance.

- Cloud computing

Cloud computing offers compelling economic advantages for financial institutions when compared to their legacy and centralised architectures. In fact, migrating the workload to cloud offers significant benefits in terms of flexibility and scalability, and allows financial institutions to innovate faster, gain efficiency, reduce time-to-market and improve productivity exponentially. Cloud computing also allows a shift from capital expenditures to operating expenses and offers means for banks to manage computing capacity to satisfy customer demands at peak periods. From this, it is evident that cloud computing is not only beneficial for incumbent banks, but that it has become essential for banks to survive and thrive in the current ecosystem, in which they face competition from digital players (either bigtech companies or smaller new entrants) that have constructed their business on cloud.

However, currently there are several regulatory and supervisory obstacles that might have contributed to the slower adoption of cloud among banks. A key concern refers to the lack of harmonisation in regulatory approaches to cloud across jurisdictions. This creates inefficiencies, especially for banks operating cross-border and given that the successful development of cloud depends to a large extent on the ability to reach economies of scale. The latter is not only an issue for incumbents, but also for new entrants, many of whom are cloud-native, who may experience barriers to growth as they keep gaining scale. Furthermore, banks face a high level of regulatory uncertainty regarding the outsourcing to cloud, and this is often related to lack of clarity on the methods banks have to comply with in order to ensure security and privacy, burdensome or unclear notification requirements or the need to ensure that contracts accommodate the rights of regulators and supervisors to access and audit relevant data.

Therefore, in order to support and facilitate the necessary adoption of cloud computing within the banking industry, financial regulators and supervisors should harmonize and clarify regulatory requirements in relation to cloud. In doing so, they must ensure that the principle “same activity, same risks, same regulation” prevails and that regulation focuses on the effects of the technology, and not on the technology itself.

BCBS Recommendation 4: *Banks should ensure they have appropriate processes for due diligence, risk management and ongoing monitoring of any operation outsourced to a third party, including fintech firms. Contracts should outline the responsibilities of each party, agreed service levels and audit rights. Banks should maintain controls for outsourced services to the same standard as the operations conducted within the bank itself.*

BBVA Comments on Recommendation 4:

Financial institutions often face high levels of uncertainty as regards supervisory expectations when outsourcing. As brought forward in Recommendation 3, this often relates to how supervisors expect financial institutions to manage, monitor and control outsourcing risks. In this sense, while we broadly agree with the last sentence in Recommendation 4 in that the responsibility for outsourced functions must be retained by the outsourcing institution, more clarity on which are acceptable means for banks to ensure control of outsourced activities would be desirable.

In this regard, and completing our comments to Recommendation 3, we would like to bring forward the following proposals as regards outsourcing:

- List of providers and/or services (not) suitable for financial outsourcing: If Supervisors are capable to establish a pre-approved list of providers and other list with no-authorized providers, this would help banks and supervisors to be more confident and efficient.

- Contracts: Similar to last proposal, standard clauses/models in outsourcing contracts would produce the same effects in banks and supervisors.

- Notification: The requirement of notification must be as harmonised and streamlined as possible. Notification should take place once the project is in the production phase in order to expedite this notification and not be a cause of delay and/or undesirable costs for the project. Moreover, supervisors must be flexible. For instance, when a similar service has been outsourced and notified, the notification requirements must be relaxed or avoided.

- Materiality assessment: Requirements to notify supervisors should distinguish between critical and non-critical functions, even if the financial institution is always required to include the outsourcing in its control framework. For this, regulators should provide a closed list of criteria (clear, principle based, technology agnostic and future-proof) to evaluate the materiality of a service.

- Physical access and audit rights. Physical access to data is not coherent with the distributed nature of cloud services. Thus, regulatory requirements should focus on ensuring access to data from the geography of the outsourcing financial entity and not on location of data that is already regulated by applicable data privacy regulations.

- Certifications: Third Party certifications of technological vendors recognized by relevant regulators. For the sake of transparency, there should be a public register of the recognized certifications and the conditions under which they would be accepted. The scope of certifications is also an important element to determine.

- Chain outsourcing: It is impossible to control the whole outsourcing chain. However, banks can include a clause in contracts whereby if the vendor is unable to include any of these obligations in its own outsourcing contracts or the same level of compliance or security cannot be guaranteed, the financial institution should be informed in advance by the vendor, having the possibility to cancel or request a modification of the service at no cost before the chain outsourcing is enforced. Thus, the ability to assess the risk impact of the chain outsourcing should be an option contractually agreed, which the outsourcing company decides to invoke or not once the information provided by the vendor is assessed according to outsourcing company's own risk appetite.

- Outsourcing by institutions with cross-border activity. In the case of financial groups with branches and/or subsidiaries in third countries, outsourcing by these branches/subsidiaries must be ruled by local outsourcing and data protection rules, whenever these exist, and not by those applicable in the home country.

Finally, in addition to the above proposals, we would like to highlight that banks are subject to stricter requirements in terms of internal policies and notification/authorization from supervisors than other players, such as bigtech companies, when partnering with fintech companies. This is also a source of unleveled playing field, since banks often face difficulties in performing the required due diligence when the chosen partner outsources functions on its own.

BCBS Recommendation 5: *Bank supervisors should cooperate with other public authorities responsible for oversight of regulatory functions related to fintech, such as conduct authorities, data protection authorities, competition authorities and financial intelligence units, with the objective of, where appropriate, developing standards and regulatory oversight of the provision of banking services, whether or not the service is provided by a bank or fintech firms.*

BCBS Recommendation 6: *Given the current and potential global growth of fintech companies, international cooperation between supervisors is essential. Supervisors should coordinate supervisory activities for cross-border fintech operations, where appropriate.*

BBVA Comments on Recommendation 6:

We completely agree with Recommendations 5 and 6, since an open dialogue between all stakeholders is essential to understand the current digital transformation and to gather evidence to support the creation of future policies. Cooperation and collaboration among regulatory authorities is essential cross-sectorally (including non-financial regulators such as data protection authorities, consumer protection authorities, and other digital-related bodies) and across jurisdictions. International cooperation is necessary because technological solutions (Cloud, blockchain,…) carry us to look for global cooperation between supervisors.

The latter is not only applicable for fintech-related innovations, but also for bank regulation and supervision. Nowadays, the international cooperation between supervisors is based in bilateral MoU´s. Even when this MoU exists, the international cooperation between supervisors could be better.

Finally, it is essential to establish a continuous and open dialogue that incorporates also the private sector. Therefore, any measures aiming at enhancing public-private cooperation are welcomed, such as the introduction of innovation hubs, accelerators or regulatory sandboxes (see our comments to recommendation 10).

Any approach that does not draw from this collaborative mindset would not be able to ensure that risks are adequately understood and mitigated, and would impede the achievement of a true level playing field across players and borders.

BCBS Recommendation 7: *Bank supervisors should assess their current staffing and training models to ensure that knowledge, skills and tools of their staff remain relevant and effective in supervising new technologies and innovative business models. Supervisors should also consider whether additional specialised skills are needed to complement existing expertise.*

BBVA Comments on Recommendation 7:

For the dialogue and cooperation mentioned in Recommendations 5 and 6 to be effective, regulators and supervisors need to invest in new skills. It is important for the institutions to build up a solid base of knowledge to allow them to understand and manage the types of issues that could arise in the new environment in the most efficient manner possible, as often these are new topics for which there is simply no previous experience to call upon.

This can be achieved through training of staff and a targeted recruitment policy. Regarding the latter, however, and given the kind of professional needed, which should have a transversal profile and is highly demanded, bank supervisors may encounter severe difficulties for attracting and retaining staff. This is a problem also for banks, who face hurdles arising from some prudential regulations on top of that. For instance, remuneration rules under the European CRD/CRR framework set a limit to the ratio between the variable and the fixed salary that financial institutions can pay to certain staff members identified as risk takers. This prevents European banks from hiring digital talent on equal footing than other sectors or banks in other jurisdictions.

BCBS Recommendation 8: *Supervisors should consider investigating and exploring the potential of new technologies to improve their methods and processes. Information on policies and practices should be shared among supervisors.*

BBVA Comments on Recommendation 8:

We also see potential in the use of new technologies to enhance supervisory procedures and processes. In relation to recommendation 7, developing new skills and capabilities would also allow authorities to maximise the new opportunities that technological innovation offers. The development of regtech and suptech solutions can provide benefits to the whole financial services industry and to the authorities, as it eases the relationship among them and facilitates the process of reporting and monitoring. As already commented, recent work by the Institute of International Finance on regtech could be of interest to the BCBS and national supervisory authorities (please refer to recommendations 1 and 2).

BCBS Recommendation 9: *Supervisors should review their current regulatory, supervisory and licensing frameworks in light of new and evolving risks arising from innovative products and business models. Within applicable statutory authorities and jurisdictions, supervisors should consider whether these frameworks are sufficiently proportionate and adaptive to appropriately balance ensuring safety and soundness and consumer protection expectations with mitigating the risk of inadvertently raising barriers to entry for new firms or new business models.*

BBVA Comments on Recommendation 9:

The digitalization of financial services generates new risks, or may change the nature and reach of existing ones, which are not fully covered by traditional regulatory and supervisory approaches, and that have implications on the traditional objectives of financial stability, financial integrity, efficiency and consumer protection. Therefore, we support the need to review the existing regulatory, supervisory and licensing frameworks.

To this end, we support the design and implementation of narrow fintech licences for specific activities, as long as the level playing field is ensured. These licences should be activity and risk specific (otherwise, a generic FinTech license would practically equal a banking license) and banks should be allowed to perform any of the activities regulated under narrow fintech licenses. This is particularly useful in areas where market developments have not been followed by a thorough risk analysis and, the case being, appropriate regulation (such as crowdlending, financial services marketplaces or virtual asset management). Anyway, this authorization to provide a specific service should not be understood as a shortcut to provide additional services outside the scope of the initial license.

Furthermore, as addressed in the General remarks, a lack of regulation of some services or business models does not only point to the possibility of unaddressed risks in the financial system, but also to the existence of an unleveled playing field among different players, as regulated players often face obstacles to engage in non-regulated activities. Incumbent institutions are subject to regulatory frameworks that affect the provision of many of their services.

Finally, in the review of current regulatory, supervisory and licensing frameworks must ensure that the new framework would not constrain banks who want to embrace a digital transformation themselves. The establishment of regulatory sandboxes can help achieve these objectives.

BCBS Recommendation 10: _Supervisors should learn from each other's approaches and practices, and consider whether it would be appropriate to implement similar approaches or practices._

BBVA Comments on Recommendation 10:

First of all, as commented before, in highly regulated industries such as financial services, compliance requirements and regulatory uncertainty hinder innovation. Therefore, measures such as innovation hubs, accelerators or regulatory sandboxes are welcomed, as they can help reduce the cost and time to innovate. Furthermore, these initiatives contribute to enhance public-private collaboration, as well as collaboration among different authorities. Nevertheless, these public actions should not substitute private-led initiatives in which supervisors can also take part.

Regarding regulatory sandboxes, we believe that, if adequately implemented, they offer promising benefits for all the involved parties: for regulators and supervisors, regulatory sandboxes facilitate the understanding of costs, risks and opportunities of new solutions; consumers will enjoy the benefits of efficiency gains and will gain access to a broader range of innovative solutions; fintech startups will benefit from lower initial one-off burden of regulatory requirements; and finally, incumbent banks can benefit from lower costs and delays of innovation. Sandboxes offer financial entities the possibility to bolster their innovation projects and learn faster, while at the same time fine-tuning their value propositions.

In order to fully capture the aforementioned benefits and in light of the evidence raised by both the BCBS and the EBA as regards differences in jurisdictions' approaches to regulatory sandboxes and similar initiatives, we would see merit in achieving some harmonisation at international level, for instance through the identification of general principles. In our view, the following principles should govern the design of a regulatory sandbox:

- Regulatory sandboxes should be ruled by clear ex-ante principles to ensure fairness and avoid arbitrariness. Yet flexibility is also needed to quickly address the specificities that are inherent to any innovation.

- The sandbox must ensure a level playing field between new players and established firms that are already authorised. Therefore, participation in the sandbox should be voluntary and open to all parties. To achieve a true level playing field, a minimum set of requirements should be established for all participants.

- Different regulatory and supervisory bodies (prudential, consumer protection, data protection, AML/CFT, etc.) should be involved to ensure the sandbox is really effective.

- Sensitive data about the innovations that apply and/or participate in the sandbox should remain confidential between the firm and the authorities.

- Fundamental customers' rights and the integrity of the financial system should never be eroded during the sandboxing activities.

In order to achieve a common definition for regulatory sandboxes, some degree of homogeneity is needed in the definition of criteria to enter the sandbox, in the internal operative and, finally, in the conditions under which the exit will take place.

- To enter the sandbox, at least one of the following reasons must be met:

    - There is uncertainty on how the existing regulatory framework applies. This may be the case, for instance, for applications of distributed ledger technologies.

- Approval requirements from regulatory or supervisory bodies delays testing with real customers (for instance, a new identity verification method)

- Complying with all the regulatory obligations is too costly and time consuming just for testing. This may be the case in the process of a creating a new venture firm that meets all licensing requirements.

- The innovation would breach rules that are not fit in the current market. This refers, for example, to requirements to obtain and record physical copies of IDs in digital onboarding processes.

- Once in the sandbox, the company who has entered the sandbox must accept testing conditions that imply no detriment of consumer rights, must prove that the proposition will not affect the open economy, and report to the regulator according to a previously agreed roadmap.

- Exiting the sandbox is a key milestone in the process, as the final objective is that the project should enter the market under clear regulatory conditions. If regulatory change is needed, this possibility should be assessed and eventually undertaken by the regulators.

In conclusion, regulatory sandboxes can help to foster innovation but must be considered an exceptional process that cannot be understood as a shortcut to avoid regulation for any given project, as this could be against the principle of creating a level playing field for all stakeholders.

BBVA

For further information, please contact BBVA's Digital Regulation Unit

Lead Economist for Digital Regulation

Álvaro Martín
alvaro.martin@bbva.com

CONTACT DETAILS: BBVA Research: Azul Street, 4. La Vela Building – 4th and 5th floors. 28050 Madrid (Spain).
Tel.: +34 91 374 60 00 y +34 91 537 70 00 / Fax: +34 91 374 30 25 - www.bbvaresearch.com