BBVA | RESEARCH

Digital Economy Outlook

APRIL 2016 | DIGITAL REGULATION UNIT

Index

Summary

The Open Banking Standard: defining the API bank model

UK authorities are leading regulatory initiatives to promote greater innovation and competition in financial services by leveraging the digital opportunity. Regulating data sharing and banking APIs is currently on the regulator's agenda due to their potential benefits both for consumers and financial institutions. Defining a solid framework for banks to share information and products would place the UK in a strong position to lead the development of an international standard.

Global regulators and digital financial inclusion: an evolving landscape in need of close attention

The digitization of financial services is increasingly regarded as a decisive factor in the promotion of financial inclusion. The risks and rewards of this development, as well as its implications for the work of the global standard-setting bodies are addressed in a new White Paper issued by the Global Partnership for Financial Inclusion in March 2016.

Network Information Security (NIS) Directive

In 2013 the Commission put forward a proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union. Two years later, the Parliament and Council agreed on the text of the Network and Information Security Directive (NIS).

China's digital landscape: a digital kingdom ruled by three kings

China's digital market resists global digital players like Google, Amazon, and Facebook, as three local giants (Alibaba, Tencent and Baidu) rule the digital market through their de-facto control of the ecosystem. Now they are also entering financial services.

Unicorns: the biggest emerging companies

For the past ten years technology startups have been reaching record investment figures. Prominent among these firms are those that have attained valuations of more than US$1 billion, popularly known as unicorns. What sort of firms are they?

1 The Open Banking Standard

Defining the API bank model

UK authorities are leading regulatory initiatives to promote greater innovation and competition in financial services by leveraging the digital opportunity. Regulating data sharing and banking APIs is currently on the regulator's agenda due to their potential benefits both for consumers and financial institutions. Defining a solid framework for banks to share information and products would place the UK in a strong position to lead the development of an international standard.

Context

In September 2014, HM Treasury published a report on data sharing and open data for banks[1], which explored potential uses of data in financial services through Application Programming Interfaces (APIs) in financial services, in a way that is consistent with data protection and privacy.

In March 2016, the British Open Banking Working Group (OBWG) released a document on The Open Banking Standard[2] in response to a previous request made by HM Treasury in September 2015. The document defines a framework for an open banking model and addresses how data should be created, shared and used by its owners and those who can access them.

The latest European Directive on payments (PSD2), released in January 2016, requires banks to provide services that will enable their customers to receive some of their data over the Internet and easily, safely and securely share it with third parties, when it enters into force in 2018. The upcoming General Data Protection Regulation (GDPR) will enshrine the individual's rights to data portability, consent to sharing and specific uses. Implementing the Open Banking Standard framework could significantly accelerate the implementation of new EU regulations on banking data.

Platform banking, in which external developers can use APIs to create and extend new services, has the potential to completely reconfigure the value chain and the business model of financial institutions.

The Open Banking Standard framework

The mission statement of the Open Banking Standard (OBS) is defined as 'unlocking the potential of open banking to improve competition, efficiency and stimulate innovation in the banking sector', and the OBS document also addresses key issues around usability, trust, security and governance of the standard.

The document provides a clear definition of the main concepts involved in the API data sharing model (figure 1):

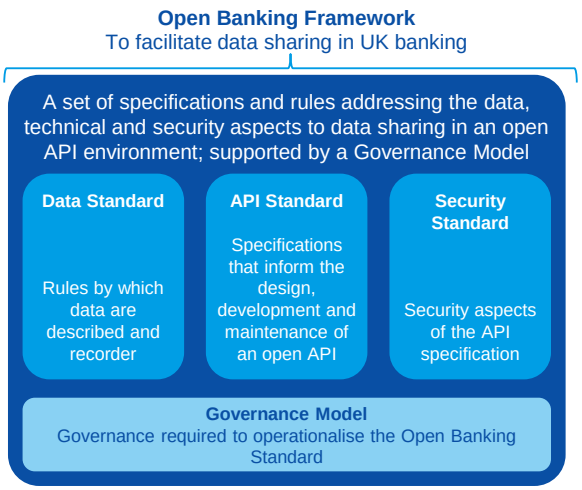
- First of all, it defines standards and a taxonomy of data for banking transactions and clarifies the uses and ownership of data in each case. Open data, shared data and private data can be generated by banking transactions (figure 2).
- Secondly, it defines open APIs or open standards, in which the technology and the standard are open but private data can only be accessed with permission from the data owner. Requirements for scalability, data architecture and resources for developers are also defined in the document. The focus is on openness and usability for developers, using existing resources that are already standards (such as OAuth).
- The OBS also defines the security aspects of API specifications, including authentication, authorisation,

1: Open Data Institute and Fingleton aasociates, *Data sharing and open data for banks*, HM Treasury and Cabinet Office, London, 2014 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/382273/141202_API_Report_FINAL.PDF
2: *The open banking standard*, Open Banking Working Group, London, 2016 https://www.scribd.com/document_downloads/298569302

access levels and permissions, and encryption, as well as security standards for data attribute providers and third parties.

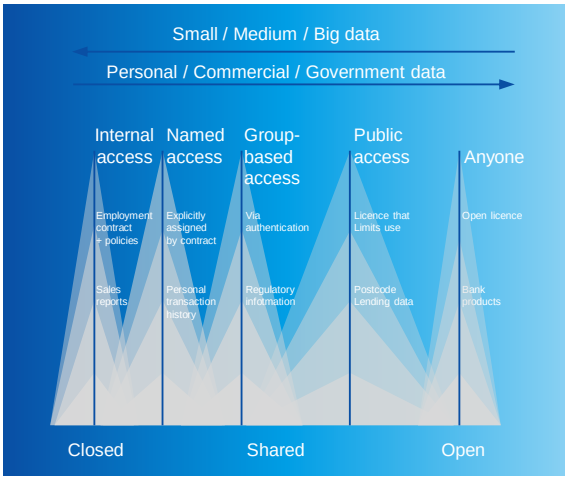
- The governance model for the ecosystem should include the creation of an Independent Authority to ensure that standards and obligations between participants are upheld.

Figure 1.1
The open banking framework



Source: Open Data Institute

Figure 1.2
The data spectrum



Source: Open Data Institute

Potential uses and challenges

By improving access to APIs and data, a more diverse ecosystem of third parties will be bred. The participation of new players will lead to greater product innovation and choice for consumers. The standard is necessary to eliminate frictions and allow economies of scale and scope.

Data sharing for specific purposes during the "customer journey" allows, for example:

- The development of new services, such as comparing current accounts and personal financial management tools.
- Improved access to credit for individuals and SMEs as they can easily share historical transactional data with lenders.
- Simpler online accounting for SMEs, directly extracting the data they need for bookkeeping instead of inputting the data manually.
- Fraud detection can be facilitated by monitoring data across multiple accounts to identify patterns.

Today, the main challenges around the OBS are centred on security, the customers' data literacy regarding adopting the proposition and addressing forthcoming legal and regulatory frameworks. Defining the framework is the first step toward mobilising the stakeholders and moving the OBS forward.

Roadmap

The proposed implementation plan has an ambitious timeline, as it aspires to cover the full extent of its scope in time for PSD2 to come into force. The aim is to have a Minimum Viable Product by the end of 2016 that can offer basic read access to data.

The API model is affected by a number of existing legal and regulatory requirements (such as the Data Protection Act - DPA - in the UK, GDPR in the EU, competition and intellectual property laws and the current Payment Services Directive), which should be considered in the implementation.

Conclusion

The use of APIs to share bank data using third-party software applications is mandatory in order to comply with existing and possible forthcoming regulations. The use of APIs by banks is becoming increasingly common as they help to drive speed and cost-effectiveness compared to traditional legacy systems.

Technology companies have used API strategies to create ecosystems that grow their product offering in new ways at a low cost. Developing an Open Banking Standard would allow banks to extend their traditional business, by becoming API providers, financial services platforms or both.

Regulation should ensure that the development of these business models achieves a high level of security, financial stability and consumer protection. The definition of the standard is a necessary step in the implementation of the model, and the UK Government, by commissioning this report, has taken the lead for future developments.

2 Global Regulators and Digital Financial Inclusion

An evolving landscape in need of close attention

The digitization of financial services is increasingly regarded as a decisive factor in the promotion of financial inclusion. The risks and rewards of this development, as well as its implications for the work of the global standard-setting bodies are addressed in a new White Paper issued by the Global Partnership for Financial Inclusion in March 2016.

The strong commitment of the G20 to promoting financial inclusion has prompted the increased involvement of other global standard-setting bodies (SSBs)[3], national legislators and industry participants. At the same time, financial and non-financial institutions have begun to offer new digital financial services with the objective of reaching millions of new customers. While global regulators come to appreciate the huge potential of these new digital financial services in promoting financial inclusion, they are also realizing that the nature of the risks faced will change along the way.

In March 2016, the Global Partnership for Financial Inclusion (GPFI) released a White Paper trying to raise awareness of this changing landscape. It provides guidance on how SSBs can strike the right balance between promoting digital financial inclusion and the traditional objectives of safeguarding financial stability, ensuring financial consumer protection and maintaining financial integrity. Establishing an enabling regulatory framework compatible with the traditional mandates of financial regulation is a responsibility that lies mainly at the national level. Still, work by the SSBs represents a significant step forward and can guide member and non-member countries in addressing the financial inclusion challenge.

Digital financial inclusion: the state of the art for global financial regulators

According to the GPFI, digital financial inclusion refers to the use of digital financial services to promote financial inclusion. It involves the use of digital means to reach financially excluded and underserved populations with a range of formal financial services suited to their needs, and at a cost that is affordable for the customers and suitable for the provider.

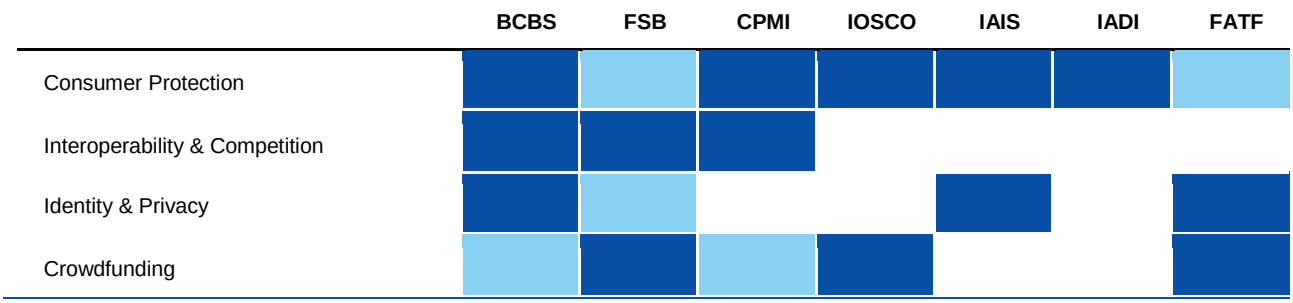
Several factors can explain the different nature of risks created by digital financial inclusion. First, the involvement of new providers requires establishing proportionate regulatory and supervisory requirements in a way that protects the level playing field. Second, new products and services are offered (in many cases, bundled together). These are often based on cutting-edge technology that may vary in quality, thus raising data security issues. Finally, there is the profile of the customers themselves, who most likely will lack experience with formal financial services, thus leading to a greater consumer protection challenge. Digital financial inclusion affects several cross-cutting issues that relate to the core mandates of global SSBs:

- **Financial consumer protection.** Financial inclusion already presents a challenge for consumer protection due to the nature of the target customers themselves, but the risks escalate when the digital dimension is added into the equation. To give an example, the use of digital transactional platforms (which combine features of payments and value-storing instruments) and the financial services that can be offered via these platforms raise several issues regarding consumer protection that are of interest to BCBS, CPMI, IADI, IAIS and IOSCO. Consumer protection also matters to the FSB and the FATF due to the link with financial stability, misconduct and financial integrity.

3: The White Paper considers the work of the primary SSBs, which include: the Basel Committee on Banking Supervision (BCBS), the Financial Stability Board (FSB), the Committee on Payments and Market Infrastructures (CPMI), the International Organization of Securities Commission (IOSCO), the International Association of Insurance Supervisors (IAIS), the International Association of Deposit Insurers (IADI) and the Financial Action Task Force (FATF).

- **Interoperability and competition:** in the presence of banks and non-banks (including Mobile Network Operators), ensuring that customers of competing financial services are able to operate with each other is a matter of utmost importance. On this matter, the hurdle is deciding on the type and timing of regulatory intervention. Increased competition can broaden the offer of products and services and lead to lower costs. At the same time, it is essential to ensure that proportionate regulation for different providers follows a risk-based approach that guarantees a level playing field between actors that engage in similar activities. Both the BCBS[4] and the CPMI have made a lot of progress on this front.
- **Customer identity and privacy:** New technologies used in digital financial inclusion (e.g. new data sources and data processing practices) facilitate the implementation of simplified CDD measures (as mandated by the FATF), thus helping to achieve a balance between the objectives of financial inclusion and integrity. At the same time, these practices also raise new issues regarding data privacy and security, as more institutions and individuals now handle personal data. Data privacy and security breaches increase the risk of identity fraud and undermine consumer confidence, to the detriment of financial inclusion.
- **Non-traditional financial intermediation:** The challenge regarding crowdfunding and other forms of P2P lending is to encourage innovative funding sources that complement bank-based finance while ensuring effective investor protection. Thus far, regulatory regimes for crowdfunding are in their infancy and none of the SSBs has yet issued guidance on this, although the issue touches upon the core mandates of several SSBs.

Table 1
Selected issues on digital financial inclusion: relevance to global SSBs



Source: BBVA Research based on the GPFI White Paper and information provided by the SSBs
Dark blue: directly relevant to the SSB's mandate. Light blue: indirectly relevant

Financial supervisors may face significant operational constraints and often lack sufficient expertise to deal with this increasingly complex reality. Digital financial inclusion therefore calls for strong cooperation and coordination among financial and non-financial authorities to ensure that the rules are consistent and coherent.

4: See related BBVA Research Watch: BCBS Guidance on regulation and supervision for financial inclusion

3 Network Information Security (NIS). Part 1 of 2

Cyber security regulation

In 2013 the European Commission put forward a proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union. Two years later, the European Parliament and Council agreed on the text of the Network and Information Security Directive (NIS).

Context

After various analyses and surveys carried out in the European Union regarding cyber security, the necessity for Network Information Security (NIS) originated in 2002. Back then, the security of information networks was determined as important, both at the economic and social level. An increasing frequency of cyber incidents was then detected. Furthermore, it became evident that the Internet connected the Member States in the same way that roads link cities and countries together, allowing the free flow of goods and services. Therefore, to secure the future of the Digital Single Market project, it appeared essential to promote the stability and resilience of network information.

These studies made evident the concern of many European companies and governments about their dependency on digital networks and their infrastructures for the delivery of their most essential services. It was considered that an NIS incident could have an enormous negative impact if the functioning of critical services was breached. In the same manner, it was thought that such cyber security incidents would affect consumer confidence and that of society at large. Due to the large disparity in NIS capacities and in the readiness of the different Member States, a voluntary approach to NIS would not offer sufficient protection against cyber security incidents and risks. The analysis of critical infrastructure providers and essential services concluded that not all of them were subject to the same obligations regarding the adoption of security measures, such as the management of technological risk and the interchange of relevant information with the Authorities. So there was clearly a need for a common Network Information Security approach.

On 18 December 2015, the European Parliament reached an agreement, pending ratification in 2016, for the approval of the NIS Directive. This Directive aims to improve cyber security capabilities in Member States in order to create a more open, secure and resilient cyberspace. With the aim of creating a more secure European Union, it also intends to develop technological and industrial resources for cyber security, and to implement an internal market for cyber security products and services. This effort will create a space for greater collaboration between countries and companies of the European Union, which will enable the reduction of cyber-crime, preventing the fragmentation of national cyber security plans and increasing harmonization among Member States in protecting against NIS incidents, risks, and threats. Consequently, this will considerably improve protection of consumers, businesses and governments in the European Union. To this end, each country will need to define the essential service operators in the Energy, Transportation, Banking and Health sectors; and the key suppliers of digital services such as search engines and cloud computing providers. Also, it will require operators to undertake the necessary essential security measures and proceed to report significant incidents to National Authorities. Lastly, it is important that each Member State designate a competent National Authority to manage the NIS, a national Computer Security Incident Response Team (CSIRT); define national NIS strategy and a Network Information Security cooperation plan. It is important to highlight that the US Agency for Network and Information Security (ENISA) will have a key role in coordinating with other CSIRTs. Finally, it is essential that a plan be created among the Member States for cooperation with information regarding warnings and notifications of potential risks and incidents.

Issues for online businesses

Online businesses should consider five aspects of compliance and protection in their Network Information Security (NIS).

First, they should assess whether their type of company will be subject to the NIS Directive. The Directive will affect essential service operators and providers of digital services such as those in the Energy, Transportation, Financial, Hydrological, Public Administration and Health sectors. The digital infrastructure, online merchants, search engines and cloud computing services will also be affected. However, it will not affect payment service providers, which are subject to other Directives and obligations for security and notifications of cyber security incidents. Neither will hardware or software companies be affected, nor small or medium-sized businesses.

Secondly, the entity should only comply with national law transposed from the NIS Directive in the Member State where its main headquarters are based.

Thirdly, it will be crucial that the company knows what National Authority it should report cyber security incidents to, and which one could potentially exercise sanctioning power over it for any non-compliance with the law. To date, it is unclear what the powers held by the competent national Authority will be versus the national Computer Security Incident Response Teams (CSIRT). Nor is it clear what will happen with the possible duplication of incident notifications required by other Regulations already in force in some countries, such as data protection or critical infrastructures.

Fourth, online businesses or companies that need to comply with the law should protect their technical and organizational NIS measures. These measures should ensure the ability to manage security risks and threats to their own networks and information systems themselves. Companies are expected to create a culture of technological risk management that takes appropriate and proportionate measures to ensure NIS.

Finally, companies must develop an effective process for reporting cyber incidents either to the competent national Authority or the National CSIRT.

Forthcoming article will analyse the challenges that this Directive poses for regulators in different countries.

4 China's digital landscape

A digital kingdom ruled by three kings

China's digital market resists global digital players like Google, Amazon, and Facebook, as three local giants (Alibaba, Tencent and Baidu) rule the digital market through their de-facto control of the ecosystem. Now they are also entering financial services.

China's digital economy

China's digital economy is huge. There are **more than 651 million Internet users**, making up the largest online population in the world (but a penetration of barely 48%) as of February 2016[5]. **92% of these online users own a smartphone**, and each of them has on average 4.1 devices connected to the Internet. In 2015 e-commerce volume reached $589 billion, making China **the largest e-commerce market in the world**, with roughly a 40% share of the total volume[6].

The Chinese digital market has some singular characteristics. For example, **it has an entirely different set of online service providers from the rest of the world**. Facebook, Twitter, Instagram, YouTube and many other major online services are not accessible from China. And few people use Whatsapp or PayPal. There are Chinese companies that operate comparable services and foreign Internet companies have had very little success in China so far. Instead, **three big local digital players – Baidu (search engine), Alibaba (ecommerce platforms Tmall and Taobao), and Tencent (social apps WeChat and QQ) – collectively known as BATs, dominate the market**. The aggregate market value of the three companies is $473 billion and their combined annual revenue $20 billion.

BATs are so powerful in China that their mere existence sometimes prevents competition from emerging and they have become crucial players in the Chinese economy. **Their core businesses differ but they increasingly compete with one another, creating formidable Internet ecosystems within China.** Another digital disruptor is the fast-growing smartphone maker, Xiaomi, which has the potential to build a fourth major ecosystem.

There are big cultural differences in consumer behaviour too. **Chinese consumers' sensitivity to price is still more acute than we are used to in other markets**. This phenomenon often forces companies to compete on prices alone and it sometimes creates the undesirable situation in which no one in the industry is actually making a decent profit. **Another interesting business phenomenon to bear in mind is what is called the "fans economy."** Xiaomi is a master of building a brand and achieving amazing sales results by winning customers and converting them into fans of their brand. A lot of companies are now trying to replicate Xiaomi's success in generating a fans economy.

Fintech ecosystem

In the last few years there is **huge activity in the venture capital (VC) community**. A partial explanation for this is that several of the big digital players are now at a stage in which they are looking to put excess capital to work through venture-style investments in small companies. **In 2015 BATs spent almost $15 billion in mergers and acquisitions, a figure that is expected to grow to $80 billion in 2016**[7]. This has facilitated **the surge of fintech "unicorns"** like China Internet Plus Holding (a location-based dining information and group-buying discount platform), Lufax (P2P lending platforms), Didi Kuaidi (a taxi-hailing service), DJI Innovations (a drone manufacturer) and Zhong An Insurance (online insurance).

5: http://venturebeat.com/2016/02/12/new-data-shows-the-staggering-growth-of-apps-and-smartphones-in-china/
6: https://www.internetretailer.com/2016/01/27/chinas-online-retail-sales-grow-third-589-billion-2015
7: http://www.financeasia.com/News/406399,baidu-alibaba-and-tencent-on-deal-trail.aspx

New digital banks in China

China's retail banking revenues have grown annually by 30% since 2009 and could exceed $430 billion by 2020, making the country the largest retail banking market in Asia. Meanwhile, **the retail banking landscape has faced several challenges**, including interest rate liberalization, major regulatory changes and the rise of digital finance. **Incumbent banks are losing their dominance by market share, while digital banking is going mainstream.**

The growth of digital banking is driven by two major factors: the first has to do with the changing needs and behaviour of the Chinese consumer in regard to digital banking. McKinsey found that **more than 70% of Chinese consumers would consider opening an account with a purely digital bank**, and even consider it their primary bank. The second factor has to do with regulation: in order to boost the economy and help small and medium enterprises raise funding more easily, **the Chinese government is encouraging non-government entities to invest in financial institutions, even allowing private companies to open their own banks.** In 2014, when the government announced its decision to grant ten banking licenses for private banks, the big three tech companies jumped at the opportunity.

Tencent was the first, launching in January 2015 **WeBank**, the country's first online-only bank. WeBank is mainly in the business of distributing financial products for other institutions, granting small personal loans and car loans. WeBank has grown very quickly in terms of users and assets (it is rumoured to have over 2 million users; the company does not disclose any figures) because it promotes its loan service on WeChat and QQ, the dominant social media apps in China, with 800 million users. The financial products WeBank is selling have a high rate of return and so they are often sold out in seconds.

Alibaba, that same month, launched **MYbank**, which has been working on three kinds of loans indirectly tied in with Alibaba's core business: one for people in rural areas, one for internet start-ups and one for Tmall and Taobao sellers. MYbank operates on a cloud computing platform and there is no bank staff involved in granting loans. Big data algorithms are used to calculate the loan amounts, which cannot exceed RMB 5 million. The whole process is quick and easy and, in the future, it is expected that users will only need to spend three minutes on a two-step process to get a loan from MYbank. Once the application is approved, the money will reach the user's account instantly.

Baidu followed another path: instead of applying for a banking license, in November 2015 it announced its decision to launch **Baixin Bank** by cooperating with CITIC Bank, a traditional bank. Set up by a traditional bank and a search engine giant, Baixin Bank aims to offer both online and offline services. In addition, Baidu is offering user behaviour analytics, which will not only help with risk management, but will also make personalised services feasible. In the future, Baixin Bank aims to sell financial products and grant small loans to individual clients.

Conclusion

It is still **too early to analyse how competition between traditional banks and BATs will evolve**: there is not enough information about the business development of WeBank and MYbank, and even less about Baixin Bank. But there is an interesting reflection to make from the point of view of the western world: for years it has been said that **the real threat to banks is not the fintech world but the entrance of big Internet players (such as the GAFAs: Google, Apple, Facebook, Amazon) into the financial services arena**. **China is a place where this is already happening, and lessons should be learnt from their experience.**

5 Unicorns: the biggest emerging companies

The growth of technology startups

For the past ten years technology startups have been reaching record investment figures. Prominent among these firms are those that have attained valuations of more than US$1 billion, popularly known as unicorns. What sort of firms are they?

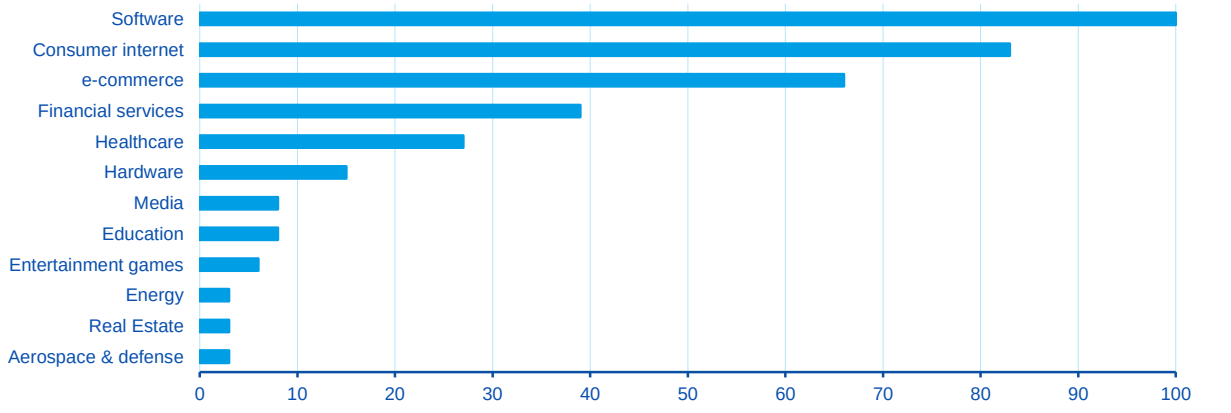
The concept

Unicorn is the name given to technology startups launched after 2003 and valued at more than US$1 billion. The term was first used in November 2013 in an article in TechCrunch[8] by venture capital investor Aileen Lee. At that time there were just 39 companies in this select group, 0.07% of the total (only considering US companies, listed and unlisted), with barely four companies a year being added to the group: they were as rare as unicorns.

Since then analysts of the startup world have not stopped talking about unicorns, and the concept has been redefined to include only companies that are not yet listed on any market and whose investors include venture capital firms not majority controlled by institutional investors. This criterion excludes the giants of the Internet, which not only surpass the unicorns' valuations but also continue to grow constantly.

We are talking about technology firms, and we see them in all sectors that have been affected by digitisation. Their model is based on disaggregating traditional companies' businesses, concentrating on only a part of a business or detecting new niches of opportunity.

Figure 5.1
Unicorns by sector



Source: BBVA Research based on data from TechCrunch

In many cases their value proposition is based on new business models within the digital economy. Only a few of these firms have a strong element of technological innovation, but all of them make use of the value of data as a differential factor. Moreover, many of them operate as platforms, defined as technological infrastructures providing a meeting point between demand for products and services and supply of contents and applications.

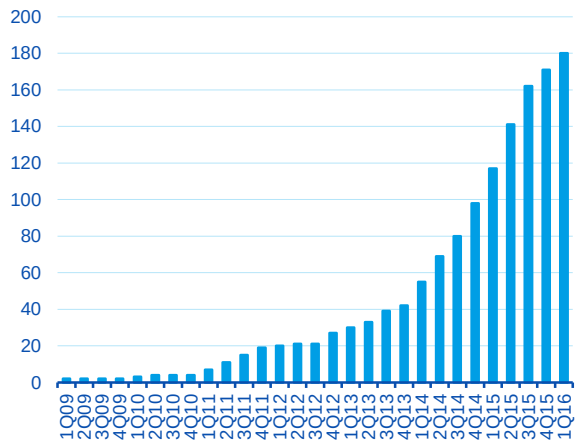
8: Lee, Aileen,"Welcome to the Unicorn Club: learning from billion dollar startups", *TechCrunch*, 2 Nov. 2013

Some figures

In April 2016 there are approximately **160 unicorns** worldwide[9], although only about 1% of all startups can aspire to become a unicorn. The time taken by a firm to become a unicorn has been getting shorter in the past three years, and 2007 is the year in which the biggest number of companies on the list were established.

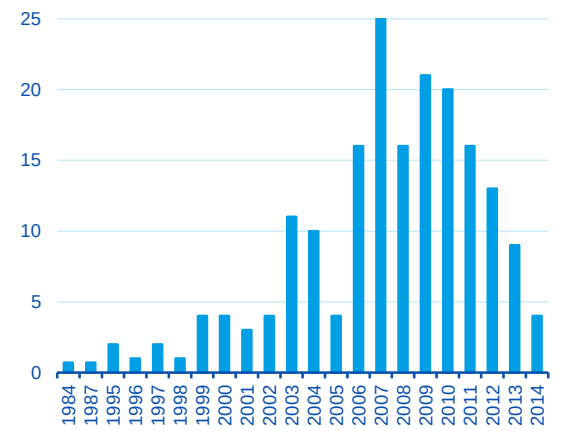
The list is headed by Uber, the transport company that does not possess a single vehicle, currently valued at US$51 billion, followed by Chinese technology firm Xiaomi, which together account for US$96 billion or 17.5% of the total of US$548 billion at which all unicorns are valued, according to TechCrunch. The "superunicorns" or "decacorns", firms valued at over US$10 billion, currently number 11, while in 2013 this threshold was passed only by Facebook.

Figure 5.2
Evolution in the number of unicorns



Source: CrunchBase

Figure 5.3
Unicorns by year of establishment



Source: CrunchBase

For the time being these companies prefer not to go public, and obtain their financing from investors who continue to bet on emerging companies as a profitable asset in an environment of very low interest rates, although to date the profits they generate do not in themselves justify the valuation. The sectors capturing most investment are evolving, and although many companies fail, the unicorns' birth rate has continued to grow until now.

Valuations are based on investments by venture capital firms, so it is not possible to see how they evolve in real time, and they may well be revised in subsequent transactions. Since they are not listed on organised markets, these firms are not obliged to publish their accounts, and their value is estimated on the basis of business prospects using data such as the number of users or the potential of the markets in which they operate. We find a considerable number of cases in which the valuation has declined from one financing round to the next, or upon listing[10], which gives rise to doubts as to how realistic the attributed values are and to fears of the bursting of another bubble. One of the most recent cases was the initial public offering (IPO) of Square, in November 2015. Its initial estimated value had been US$6 billion, but the IPO eventually priced it at US$2.9 billion[11].

9: As at 31 March 2016 according to TechCrunch there were 162 (*Crunch Base Unicorn Leaderboard*), while CBInsights counted 159 (*The unicorns list*) and DowJones VentureSource (The Billion Dollar Startup Club) reported 146.
10: Updated information can be found at CBInsights' *The downround tracker*
11: "Square's disappointing IPO shows the risk of overvaluing tech unicorns", *The Economist*, 19 Nov. 2015

The unicorns' natural **habitat** is Silicon Valley, which was first given this name in 1971 and where the main companies of the Internet age have been based. Indeed, most of these firms are in the United States (88)[12], not just in Silicon Valley but also on the East coast, followed by China, with 40. In Europe the number is smaller (16), possibly due to the greater degree of market fragmentation and the regulatory barriers that still limit the growth of startups on this side of the Atlantic. Moreover, the limited tax incentives for investing in this kind of firm, together with the constraints of European labour legislation when it comes to attracting talent, pose further difficulties in competing with other parts of the world. In the United States, the JOBS (Jumpstart Our Business Startups) Act of 2012, aimed at helping small startups to obtain capital, enables emerging companies to stay afloat without going public, by attracting funds from venture capital investors.

Conclusion

The unicorn concept has been used to single out companies with successful exponential growth, although debate continues on the justification for some valuations and whether they should be maintained if the company goes public. There are persistent fears that we may be looking at another bubble similar to that of the dot-com firms in the 1990s, although there is so far no certainty about this. What is true is that their growth is changing the panorama in many sectors, due to the novel nature of the business models being proposed and their interpretation of the transformational trends in the digital economy.

12: According to DowJones VentureSource, information as at 9 April 2016 (The Billion Dollar Startup Club)

DISCLAIMER

This document has been prepared by BBVA Research Department, it is provided for information purposes only and expresses data, opinions or estimations regarding the date of issue of the report, prepared by BBVA or obtained from or based on sources we consider to be reliable, and have not been independently verified by BBVA. Therefore, BBVA offers no warranty, either express or implicit, regarding its accuracy, integrity or correctness.

Estimations this document may contain have been undertaken according to generally accepted methodologies and should be considered as forecasts or projections. Results obtained in the past, either positive or negative, are no guarantee of future performance.

This document and its contents are subject to changes without prior notice depending on variables such as the economic context or market fluctuations. BBVA is not responsible for updating these contents or for giving notice of such changes.

BBVA accepts no liability for any loss, direct or indirect, that may result from the use of this document or its contents.

This document and its contents do not constitute an offer, invitation or solicitation to purchase, divest or enter into any interest in financial assets or instruments. Neither shall this document nor its contents form the basis of any contract, commitment or decision of any kind.

In regard to investment in financial assets related to economic variables this document may cover, readers should be aware that under no circumstances should they base their investment decisions in the information contained in this document. Those persons or entities offering investment products to these potential investors are legally required to provide the information needed for them to take an appropriate investment decision.

This report has been produced by the Digital Regulation Unit:

Chief Economist for Digital Regulation Unit
Álvaro Martín
alvaro.martin@bbva.com

Vanesa Casadas
vanesa.casadas@bbva.com

Israel Hernanz
israel.hernanz@bbva.com

Alicia Sánchez
alicia.sanchezs@bbva.com

Javier Sebastián
jsebastian@bbva.com

Pablo Urbiola
pablo.urbiola@bbva.com

With the contribution of:

Francisco Borja Larrumbide Martínes
fborja.larrumbide@bbva.com

Lucía Pacheco
lucia.pacheco@bbva.com

BBVA Research

Group Chief Economist
Jorge Sicilia Serrano

Developed Economies Area
Rafael Doménech
r.domenech@bbva.com

Spain
Miguel Cardoso
miguel.cardoso@bbva.com

Europe
Miguel Jiménez
mjimenezg@bbva.com

US
Nathaniel Karp
Nathaniel.Karp@bbva.com

Emerging Markets Area

Cross-Country Emerging Markets Analysis
Alvaro Ortiz
alvaro.ortiz@bbva.com

Asia
Le Xia
le.xia@bbva.com

Mexico
Carlos Serrano
carlos.serranoh@bbva.com

Turkey
Alvaro Ortiz
alvaro.ortiz@bbva.com

LATAM Coordination
Juan Manuel Ruiz
juan.ruiz@bbva.com

Argentina
Gloria Sorensen
gsorensen@bbva.com

Chile
Jorge Selaive
jselaive@bbva.com

Colombia
Juana Téllez
juana.tellez@bbva.com

Peru
Hugo Perea
hperea@bbva.com

Venezuela
Julio Pineda
juliocesar.pineda@bbva.com

Financial Systems and Regulation Area
Santiago Fernández de Lis
sfernandezdelis@bbva.com

Financial Systems
Ana Rubio
arubiog@bbva.com

Financial Inclusion
David Tuesta
david.tuesta@bbva.com

Regulation and Public Policy
María Abascal
maria.abascal@bbva.com

Digital Regulation
Álvaro Martín
alvaro.martin@bbva.com

Global Areas

Economic Scenarios
Julián Cubero
juan.cubero@bbva.com

Financial Scenarios
Sonsoles Castillo
s.castillo@bbva.com

Innovation & Processes
Oscar de las Peñas
oscar.delaspenas@bbva.com

Contact details:

Azul Street, 4
La Vela Building - 4 and 5 floor
28050 Madrid (Spain)
Tel.: +34 91 374 60 00 and +34 91 537 70 00
Fax: +34 91 374 30 25
bbvaresearch@bbva.com
www.bbvaresearch.com