BBVA | Research

Digital Economy Outlook

December 2017 | DIGITAL REGULATION UNIT

BBVA | Research

Index

Closing date: 01 December 2017

1. Summary

Digital markets: challenges for competition policy. A number of key features of digital markets - network effects, gatekeeper roles, and the use of data - have led to the rapid growth of a few big players who have accumulated power in their respective markets. This in turn has led to concerns over the need for competition authorities to act, while existing competition tools and frameworks may not be well suited to the problem.

Initial Coin Offerings (ICOs): investment in crypto tokens: fad, madness or vision? Crypto tokens issued through ICOs have gone from being below the radar at the end of 2016 to becoming the asset class with the fastest growth rate in investment volume in the history of the financial markets. However, investors must be aware of the high level of risk and the lack of specific regulation.

Towards a new digital identity: identification systems and digital environment. The economy and society are moving very fast towards a world where interactions are increasingly digital. The ability to prove that you are who you say you are is a fundamental piece of economic, financial and social development. Our current identity and data security management systems are clearly deficient, as they are still largely based on the physical world. Private companies, governments and regulators are searching for comprehensive solutions that enable clients and citizens to identify themselves.

Fintech: implications for regulation and supervision. The regulatory debate gains momentum. During 2017 financial regulators and supervisors have released several consultations and reports on the impact of financial technology (fintech) on the financial sector. This article analyzes authorities' priorities and major concerns and discusses what is needed to go forward.

Artificial Intelligence: a policy approach. Artificial Intelligence is one of the buzzwords of the moment. It is fairly clear that this disruptive technology will noticeably affect the economy and society. Although the exact impact remains to be seen, authorities are trying to understand the potential effects of this technology and devising their initial regulatory strategies.

2. Digital markets

Challenges for competition policy

A number of key features of digital markets - network effects, gatekeeper roles, and the use of data - have led to the rapid growth of a few big players who have accumulated power in their respective markets. This in turn has led to concerns over the need for competition authorities to act, while existing competition tools and frameworks may not be well suited to the problem.

What is different in digital markets?

Digital markets are those in which digital products and services are transacted. Since the concept of digital products and services is so wide, it is useful to classify them into three broad categories to provide a more precise definition:

- **Technological layers:** physical devices (hardware) and software that are needed to consume other types of digital products and services. The most significant examples of these are personal computers, mobile phones/tablets and their corresponding operating systems.

- **Digital intermediaries:** services that provide a connection to other goods and services, either digital or physical. Examples of these include web search portals, e-commerce sites, music streaming services, hotel booking websites and riding apps.

- **Digital end-products:** goods or services that are stored, delivered and consumed in electronic format, and that are a value proposition in themselves, not just by virtue of the connection to other goods and services. This is the case of content websites, music, e-books, videos, communication services and video games.

From this classification, we can identify a number of key features that have important implications for the dynamics of competition and the structure of digital markets:

First, **many of these markets are multi-sided**, since two or more different groups of agents obtain value from becoming connected or coordinated through a platform. This is the case of **technological layers**, which connect providers of other digital goods and services with consumers, and of **digital intermediaries**, which have providers of end-products or advertisers on one side of the market and buyers/users on the other.

The defining characteristic of multi-sided markets is the presence of **indirect network effects**, which means that the benefit for agents on one side of the market increases with the number of agents on the other side. Some markets also show **direct network effects**, meaning agents value the number of other similar agents connected - for example in social or communication networks.

Network effects have two main implications. First, the optimal price structure of these markets differs from that of one-sided markets, and efficient pricing is not only based on costs. Second, self-reinforcing feedback loops between the different sides of the market lead to market concentration and might trigger a **"winner-takes-all" situation**, depending on the intensity of the network effects and on other factors, such as economies of scale, product differentiation, multi-homing, etc.

The second feature of digital markets it that the nature of some digital goods and services means they are **gatekeepers to other markets**, since they act as access facilities for products or services beyond their own markets. As a result, they may be able to exert a degree of control over those products, or use their gatekeeper position to enter the related markets. **Technological layers** are always gatekeepers, as they set the conditions on which other products and services are built and distributed (e.g. mobile operating systems with respect to communication applications, content apps or mobile payments). Some **digital intermediaries** also have gatekeeper roles as they are used as the access point to products and services beyond their markets (e.g. web search portals for media, travel bookings, shopping, etc.).

Another key feature of digital markets is the important role played by **data**, sometimes referred to as the "new oil" of the digital economy. Digital products – be they **technological layers**, **digital intermediaries** or **end-products** – generally use data as a production input and also generate new valuable data that can then further feed the production process. These data can be a source of competitive advantage for firms for several economic reasons. First, the accumulation of relevant data allows firms to improve the quality of their services and, as a result, to attract new users and access more data. Second, data already accumulated by firms can be reused to develop and/or offer other products and services. And third, it can produce lock-in effects, since product personalization and storage of personal data within a service can increase switching costs for consumers.

These features of digital markets lead to **market concentration**, particularly in the case of **digital intermediaries** and **technological layers**. This may be an efficient outcome given the strong **network effects** and **data-based dynamic economies of scale** that exist in these markets. However, since a few big digital players – generally platforms with **gatekeeper powers** – are accumulating power within and beyond their original markets, there is a risk that these players engage in anti-competitive practices to restrict competition, hindering the functioning of the markets.

Challenges for competition authorities

Competition laws prevent the use of market power to prevent rivals from contesting a firm's position. This anticompetitive conduct may take the form of agreements between firms (mergers, joint ventures, exclusive contracts, price restrictions, etc.) or unilateral practices (price discrimination, predatory pricing, tying and bundling, refusal to deal, etc.). Competition authorities look at firms' potential anti-competitive practices on a case-by-case basis, generally following four main steps:

- **Detect possible problems** through complaints and investigations, and self-notifications for mergers and joint ventures.
- **Define the relevant market** by applying quantitative tests that are generally based on prices.
- **Identify the possible anti-competitive behaviour and the market power of the firms involved** by looking at concentration measures, barriers to entry and other factors that affect market power.
- **Analyse the impact on competition** of the firms' behaviour, by applying practice-specific tests (some of them price-cost based) and taking into consideration the positive and negative effects.

While there is consensus that this framework is still relevant for digital markets, it may present competition authorities with particular challenges when trying to apply it.

First, when trying to spot a potential problem with a merger or other agreement. Existing **criteria for notifying and investigating mergers and joint ventures** can leave out the acquisition of firms with low turnover or market shares but high growth potential or access to valuable datasets.

Second, price-based tools used to define relevant markets have to be adapted for multi-sided markets, particularly when one side of the market has a **zero price**. Moreover, there is conceptual problem of how many markets should be defined in a multi-sided environment.

Third, when examining the market power of firms, the **barriers to entry** relevant in digital markets - and therefore the contestability of the market - are difficult to analyse. While development of an initial product can sometimes be done very cheaply, actually capturing market share may be much more difficult. For example, a new social network app could be launched with minimal investment and leverage cloud computing to keep running costs down. However, it would be extremely difficult to generate sufficient network effects, get hold of enough data to enhance the product offering (to users and advertisers), or find solutions to lock-in effects, to unseat incumbent players.

Fourth, arguments in response to these barriers often rest on the countervailing role of disruptive innovation in the digital sector. And this has indeed been conspicuous as digital markets have grown. Google Search took on Yahoo!, Altavista and Ask Jeeves. The social network MySpace was replaced by FaceBook. And Apple carved out a smartphone ecosystem niche through product innovation. But after a period of flux these markets may now be settling down. At what point do incumbents become so entrenched that disruptive innovation is no longer possible?

To properly address these challenges, competition authorities need to enhance their existing frameworks, both with new analytical tools and a more detailed understanding of the characteristics driving the outcomes we see today in digital markets.

3. Initial Coin Offerings (ICOs)

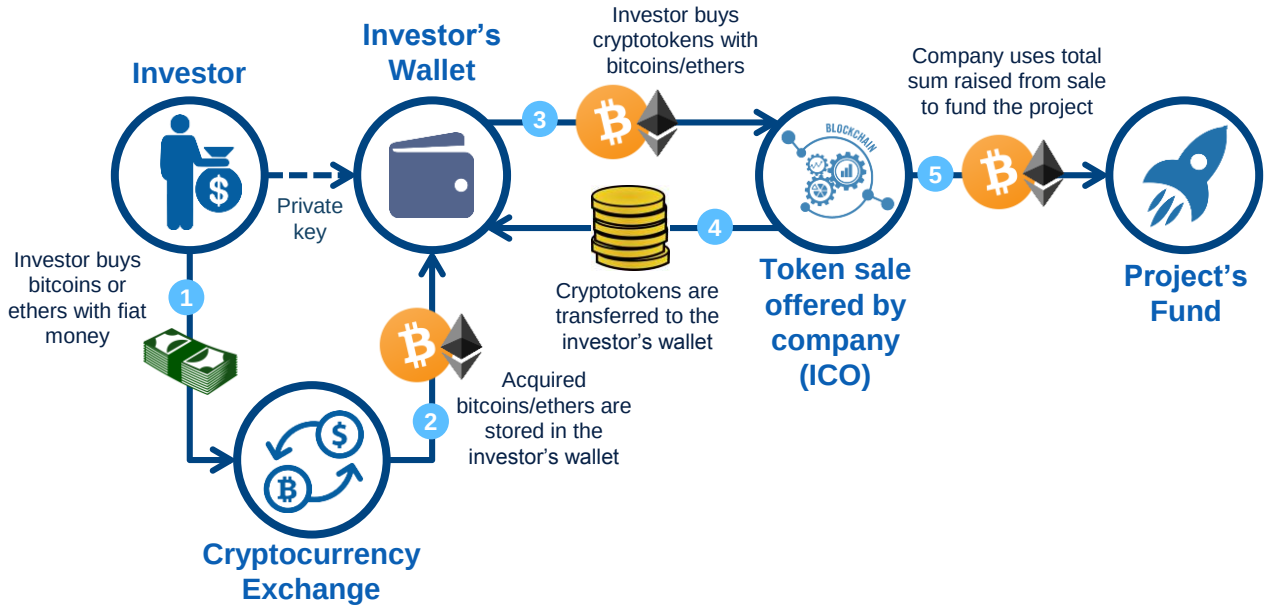
Investment in crypto tokens: fad, madness or vision?

Crypto tokens issued through ICOs have gone from being below the radar at the end of 2016 to becoming the asset class with the fastest growth rate in investment volume in the history of the financial markets. However, investors must be aware of the high level of risk and the lack of specific regulation.

What ICOs are

An ICO is a funding method for new blockchain startups based on the sale to investors of a percentage of proprietary cryptographic tokens issued by the company usually in exchange for another cryptocurrency, such as ether or bitcoin. After the offering period ends, the company is supposed to utilize the funds from the ICO to further develop its project.

Figure 3.1 Basic mechanism of an ICO



Source: BBVA Research

It has become in less than a year the preferred funding method for these companies, over the traditional alternatives offered by venture capital, banks or financial markets. For blockchain startups and projects it is an easy method of raising capital without the existence of intermediaries and mediators. Also, ICOs have allowed independent investors to participate in early-stage funding rounds of projects.

The issued tokens can be of different types and provide investors with different returns on investment. Most tokens are needed in order to use the product or service that the company is trying to develop, but do not give any sort of right of ownership or participation in future profits of the company. These are called '**utility tokens**' and the logic

behind the investment is that if the product or service is successful in the future, the value of the token will rise because of the need to use it to have access to the service. Another type of token gives ownership rights to investors in the company, so they are called '**security tokens**'. Finally, there are tokens used as mere currencies or assets (often called '**currency tokens**'), and investors buy them with purely speculative objectives based on price fluctuations.

Ethereum is the leading blockchain platform for ICOs, with more than 56% market share[1]. Unfortunately, ICOs over the Ethereum network have resulted in much phishing and many Ponzi schemes and other scams, accounting for about 10% of total ICOs[2].

How ICOs are operated

Usually, an ICO starts when a group of technologists decide to work on a project. They author a white paper that explains the technical and business dimensions of a project. Best practices include explaining how the technology works, the role of the token and its source of value, and mechanisms for issuing tokens and accessing raised funds, increasingly supported by independent audits.

Before an ICO actually takes place, there may be a pre-ICO or pre-sale. The goal of the pre-ICO period is to collect as much money from 'whales'[3] as possible. That money is typically added into the ICO or token generation contract, it acts as validation for smaller fish that "big money" is backing the project and can lead to "FOMO" (fear of missing out), which leads to an ICO hitting its cap. The very first ICOs did not have any sort of minimums or caps. ICO promoters quickly realized that by putting in what is called a "hard cap" they could drive group psychology through artificial scarcity.

Initially "whales" were mainly miners or early investors that had accumulated large amounts of cryptocurrency. Now anyone can become a "whale" by buying significant amounts of bitcoins (or ether) in the market. As their identity is unknown, it is possible that they are actually the usual venture capital or institutional investors, but this information is not disclosed.

Pioneer ICOs like Ethereum offered a bonus for early participation, which was accessible to anyone. However, early in the development of ICOs 'whales' started to demand hidden bonuses for dropping large amounts into an ICO. It is normal now for a pre-ICO (or private sale) to offer a higher discount or bonus to those willing to take the risk of giving money to an immature project.

Tokens are sold to a global crowd whose main commonality is technological literacy; there is generally no requirement to be an accredited investor or live in a particular country or region. In order to participate in an ICO the individual investor usually has to 'subscribe' during the pre-ICO period, indicating the desired number of tokens and sending the

1: *'ICO Market Research: The Leading Blockchain Platforms of 2017'*. ICO Watchlist.
2: *'Exploits, Hacks, Phishing, Ponzi Are on the Rise on Ethereum'*. The Cointelegraph.
3: individuals or groups who hold vast quantities of bitcoins.

equivalent value in bitcoins or ether to an Ethereum address provided by the issuing company. When the ICO date arrives, a smart contract distributes the issued tokens to all the addresses from which the payments were received.

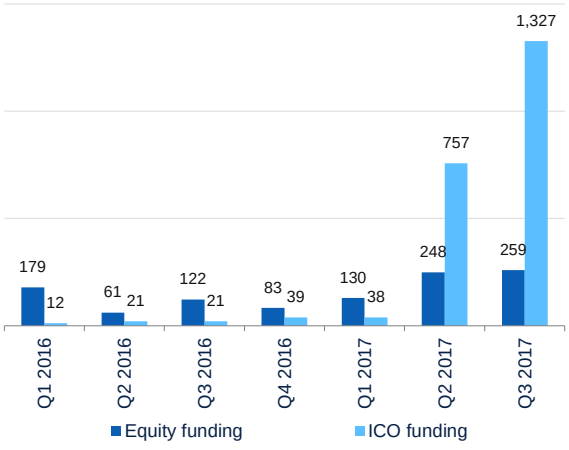
Some time after a successful issuance, the new token usually starts to list on various crypto exchanges, where a whole secondary market for crypto tokens has arisen.

ICOs compared to other funding mechanisms

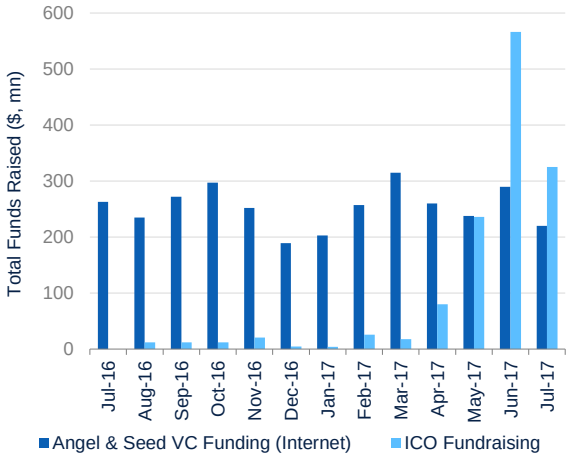
ICOs present differences with respect to other sources of corporate funding at companies' different stages, like Venture Capital or IPOs, the most important ones being that: a) they are purely peer-to-peer funding schemes, and b) they are mostly still unregulated. In any case, ICOs have been the preferred funding method for blockchain start-ups for the past year.

Figure 3.2 ICO Funding evolution

Conventional Equity Funding To Blockchain Firms Vs. ICO Funding (Global, Millions ($), Q12016-Q32017)



Angel & Seed VC Funding to startups vs. ICO Funding (Total Funds Raised by month ($ Millions))



Note: ICO fundraising as of July 18th, 2017, per Coin Schedule. Angel & Seed VC funding data as of July 31th, 2017 and does not include "crowdfunding" rounds.
Source: CB Insights, CoinSchedule, Goldman Sachs Global Investment Research

As we can see, ICOs were marginal compared to VCs for blockchain firms until Q2 2017, when the ICO craze started, and ICO funding is now five times the amount of conventional equity funding. Overall, ICO funding has also surpassed global early-stage funding (Angel and Seed VC) for start-ups since June 2017.

Regulation of ICOs

In the last six months, the volume of ICO investment and the lack of investor protection have pushed regulators all over the world to react in different ways, ranging from the total banning of ICOs to the issuing of warnings and/or guidelines for issuers and investors, and even to the development of specific regulation.

In July 2017 the U.S. Securities and Exchange Commission (SEC) indicated that it could have the authority to apply federal securities law to ICOs. The SEC stated that most tokens are equivalent to securities, and therefore issuers have to comply with the Securities Act. For other tokens issuers have to properly inform the SEC about the purpose of the token, and consumers about risks.

Following a completely different line, in September 2017 Chinese financial regulators officially banned all ICOs. South Korea followed shortly afterwards, but in both cases the ban seems to be temporary, until proper regulations have been developed.

Regulators from the UK (FCA), Germany (Bafin), Spain (CNMV), Singapore (MAS), Australia (ASIC), Switzerland (FINMA) and others have issued warnings for investors or guidelines for issuers to comply with the minimum consumer protection regulation. In France, the AMF has launched the 'Unicorn' project to develop a specific regulatory framework for ICOs and to give support to companies wishing to issue crypto tokens. Canada's Autorité des marchés financiers (AMF), the financial regulator for the Quebec region, has allowed the world's first regulated token sale within its regulatory sandbox.

Finally, the ESMA published in November 2017 one statement for investors, warning about the risks of investing in ICOs, and a second one for issuing companies, identifying the applicable regulation they should comply with.

4. Towards a new digital identity

Identification systems and digital environment

The economy and society are moving very fast towards a world where interactions are increasingly digital. The ability to prove that you are who you say you are is a fundamental piece of economic, financial and social development. Our current identity and data security management systems are clearly deficient, as they are still largely based on the physical world. Private companies, governments and regulators are searching for comprehensive solutions that enable clients and citizens to identify themselves.

Digital Identity and its management

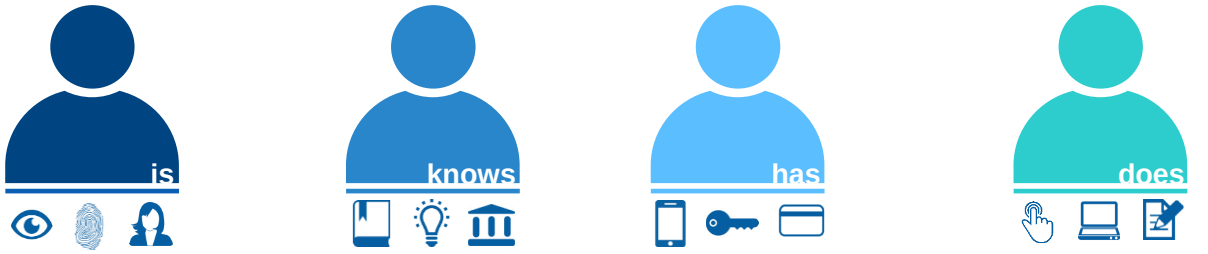
Digital identity is the digital version of a person's physical identity, the digital representation of the individual. The OECD defines Identity Management "as the set of rules, procedures and technical components that implement an organisation's policy related to the establishment, use and exchange of digital identity information."[4]

Traditional approaches to digital identity management have been focused on the creation of **static digital identities,** based on cryptographic tools, like digital signatures and digital certificates. Some of the problems of these technologies are their lack of integration with Internet-based services and also their adequacy over a long period of time, as these technologies need to be periodically verified to remain trustworthy.

The second approach is **dynamic verification**, based on an iterative process. This digital identity uses multiple sources (including, for instance, the user's mobile phone, their social media activity, geolocation, etc.). To reinforce this system's assurance level, constant assessment and monitoring is essential. These identities are usually self-asserted: it is the individual who states their attributes, and therefore the assurance level is low. **Current trends head to a combination of both approaches,** establishing a single identity for each individual based on what is known about them, something they have, what they look like or how they behave and where they live

4: "Organisation for Economic Cooperation and Development, 'The Role of Digital Identity Management in the Internet Economy: A Primer for Policymakers". OCDE 2009.

Figure 4.1



e.g.
- Age
- Gender
- Addres
- Fingerprints
- Face
- Irises
- Voice

e.g.
- Password
- Passphrase
- PIN
- Sequence

e.g.
- Access badge
- Smartcard
- Security token
- Mobile phone
- ID document

e.g.
- Motor skills
- Handwriting
- Gestures
- Keystrokes
- Applications use

Source: World Bank

Digital Identity Providers

The key issue to operate with our digital identity is the validity that others give to the veracity of the attributes of our digital identity. **A digital identity needs a provider, but, as there is no universally accepted identity supplier,** the current main providers are either public authorities (governments) that issue National eIDs to grant access to government services, or the private sector, which converts individuals into users of their systems or services, creating their own credentials (e.g. an online banking user, or a consumer of services of an online store).

Given the increasing emergence of different services that require identity validation, the current landscape demands identity systems that are able to manage identities and credentials for multiple service providers. These are the **so-called federated identity systems,** where identity information is developed and shared among several entities and across trust domains. Models of cooperation vary on the type of the project and the scope of public/private sector involvement.

Financial institutions and Identity systems

For financial institutions, identity has traditionally played a significant role in the business. In this time of transition, it is necessary for them to reach a robust, reliable and fully digital identity model that can support their current expertise in verifying identities in the analog world. Regulations have been increasingly requiring banks to perform due diligence on their customers, in an effort to trace money laundering. The pressure to comply with these regulations has meant an increased cost to banks, both in terms of money spent and internal resources dedicated to this task. There are many hurdles on the path of adapting the physical identity model to the digital one, such as lack of security, no interoperability, cyber-attacks, lack of user control over the data...

Financial institutions are currently entering the identity market as potential trusted parties in federated systems: one example is BankID, a solution developed in Sweden by a number of large banks and that can be used by members of the public, authorities and companies.

In the long term, as far as the regulation keeps adapting, for banks to become a digital identity provider it would mean investing in the trust relationship with the customers and there is an untapped opportunity to become a trusted provider across different sectors due to banks **typically being reliable by consumers above all other institutions.** After the public providers, in the private sector, banks are the most trusted, and they must take advantage of this situation. In addition, banks, due to the financial sector being so highly regulated, are used to dealing with compliance standards and can offer actors in other industries their expertise in identity-based networks.

Digital Identity challenges

As more and more users, in both their private and professional lives, rely on information they provide or which is inferred from their behaviour, remaining outside these new forms of communication is no longer a realistic option.

Users are often not aware of the extent to which the collection and use of their data is already taking place, so they are not always fully in control of their digital identity.

Security is also becoming a relevant source of concern for companies. Identity management systems are currently subject to serious liabilities such as data theft, loss or cracking of passwords, token liabilities, system hardware at risk, illicit communication monitoring and phishing. In 2016, reported data breaches[5] increased by 40%, setting a record in the US. Major hacks resulting in the release of private information are increasingly common, and identity theft is widespread. Companies like Yahoo! announced the largest data breach in history last year, affecting more than one billion accounts.

There are projects underway all over the world to try to find more trustworthy digital identity solutions and it is expected that these efforts will intensify in the next few years. On one hand**, the number of market actors that will go online is expected to grow exponentially over the next years.** On the other hand, the development of new technologies, such as the IoT phenomenon will lead to an explosion of objects, from refrigerators to shipping containers, going online as well. If all of these entities start to operate in a seamless way with each other, we will need to have standard ways of establishing and verifying who or what they are.

Legal issues

Legal certainty is important not only to assure interoperability of services across different countries and industries and consistent experiences for users, but also to provide business efficiencies and fair competition across different platforms, fostering market deployments while enabling innovation, competition and market growth.

5: The biggest data breaches in 2016. Identity Force, 2016.

Regulators must also take measures to protect consumers, **data protection** being a crucial pillar that sets the framework of a strong and secure digital identity system. It is necessary for governments to also build robust '**trust frameworks'** by regulating the different components of digital identity creation, such as technical specifications, standards and procedures.

Conclusion

The transition to a digital economy requires **different identity systems to serve different uses requiring different levels of assurance. Individuals and companies need identity solutions valid across services, markets, standards and technologies.** New technologies like blockchain, biometrics and AI can help delivery of secure identity services, in particular by governments and financial institutions, and solutions should meet the objectives of both ensuring secure identity and improving user experience.

As public identities have been created by different authorities, and since a global public identity is not a viable option in the short term, **interoperability**, or the possibility for identities generated under different identity systems to be recognized by other systems, **and collaboration between private and public entities** to offer complete solutions **is crucial.** In the long run, becoming a trusted identity provider across different sectors could represent a big business opportunity for financial institutions.

The sharing of personal data in a private, controlled, secure and convenient way, without having it spread all over the Internet, is crucial for the future development of digital identity.

5. Fintech: implications for regulation and supervision

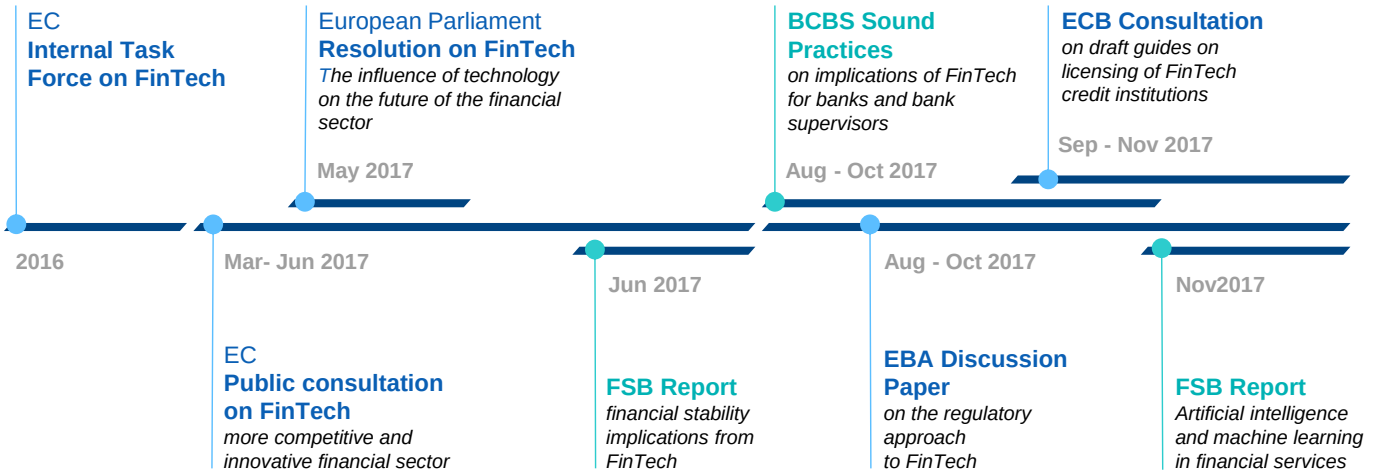
The regulatory debate gains momentum

During 2017 financial regulators and supervisors have released several consultations and reports on the impact of financial technology (fintech) on the financial sector. This article analyzes authorities' priorities and major concerns and discusses what is needed to go forward.

In Europe, the European Commission (EC) was the first body to issue a broad consultation paper assessing measures to foster the development of technology-based innovation for financial services. This document published in March is the outcome of the high-level public-private dialogue established by the EC in 2015, which resulted in the creation of an inter-services FinTech Task Force. Following the EC, the European Parliament adopted a resolution on Fintech and the influence of technology on the future of the financial sector, and more recently the European Banking Authority (EBA) stepped into the debate by issuing a discussion paper on its approach to fintech, which will serve to guide the EBA's work in the months to come. Although narrower in its scope, a recent publication of the European Central Bank (ECB) is also worth highlighting, as it represents a first glimpse of the supervisor's mindset. The ECB has recently drafted a guide to clarify the process of assessing new banking applications for institutions with a fintech business model.

However, the debate has escalated the regional level and has become central in the work of several standard-setting bodies (SSBs). In June, the Financial Stability Board (FSB) published a report analyzing the consequences of Fintech on financial stability, which has been followed by a deep-dive into the use of artificial intelligence and machine learning in financial services. Under the leadership of the FSB, other SSBs have followed. For instance, the Basel Committee on Banking Supervision (BCBS) adopted the FSB's definition of FinTech in its August Sound Practices paper**.** This discussion paper analysed the current and potential future environment for banks and bank supervisors in light of recent developments in financial innovation, and outlines 10 high-level recommendations for banks and bank supervisors.

Figure 5.1 Debate on FinTech gains momentum in 2017: Timeline



Source: BBVA Research

Different approach, same concerns

Authorities have followed different approaches and thus the follow-up is expected to differ as well. The global SSBs have developed different analytical frameworks to look at this phenomenon, arriving at high-level observations and recommendations. For instance, the Basel Committee has depicted five scenarios of the future of the banking sector depending on whether incumbent banks, small new entrants or big technological companies manage the customer relationship and ultimately provide the service. At the European level, however, the EBA and the Commission have followed a more hands-on approach that aims at defining specific policy actions. This analysis is based on an assessment of the European fintech landscape and its regulatory status. In this regard, the EBA's Discussion Paper takes stock of a mapping exercise conducted earlier in 2017 which identified that a significant proportion of the so-called fintech firms (31% of the sample[6]) in the EU are not subject to any regulatory regime or are only subject to a national authorisation or registration regime (14% of the sample).

Having said that, authorities are aligned in their analysis of the opportunities and risks arising from fintech as well as on the main concerns and priorities going forward. The latter can be summarized in the following three broad themes.

1. Understanding the change

Amid rapid technological changes and shifting customer expectations, interest in digital innovations in the financial sector is growing. Regulators and supervisors need to follow market developments to understand how the appearance of new players and the emergence of new infrastructures, products and distribution channels are going to reshape the financial system. It is reasonable to expect that new or evolving risks will appear for the system and for individual institutions. Regarding the latter, operational, IT and cyber risks have become a key concern for authorities, together with the additional pressure on the profitability of individual firms created by tougher competition.

6: The EBA has identified that there are over 1500 fintech firms in the EU, although it only has detailed information on a sample of 282 firms.

All of the above has systemic and financial stability implications as well, which may be exacerbated by an increase in market volatility and procyclicality, driven by the growing use of automated tools and services, and more concentration as a result of economies of scale and network effects. Apart from financial stability risks, policy makers are concerned about the risks posed to consumers, which may relate to data protection, financial inclusion or the ability to effectively exercise customer rights in a more complex world; and to the integrity of the financial system.

2. Assessing the adequacy of existing regulatory frameworks

International SSBs and EU bodies recognise that current bank regulatory, supervisory and licensing frameworks generally predate new technologies and business models, and this may create unintended regulatory gaps and pose undesired barriers to innovation. Going further, this may also lead to an unleveled playing field among different players. The results of the aforementioned EBA exercise are quite telling in this regard. Therefore, regulators and supervisors recognise the need to consider, within their statutory objectives and jurisdictions, whether existing frameworks are sufficiently proportionate and adaptive to reach an appropriate balance that guarantees safety and soundness and consumer protection expectations while mitigating the risk of inadvertently inhibiting innovation. As a result, they show an intention to assess whether updates of the existing frameworks are needed.

3. Defining their role

Beyond specific regulatory measures, financial authorities around the globe need to take a more pressing decision: their stance towards innovation in financial systems. Generally speaking, regulators and supervisors seek to find the right balance between guaranteeing safety and promoting innovation. In the quest for this balance, European and international policy makers are taking note of initiatives being deployed in some countries, such as innovation hubs or regulatory sandboxes, as these may help build an open dialogue between all stakeholders and provide fruitful insights into emerging models.

At the same time, however, authorities acknowledge that the global dimension and cross-sector nature of the fintech phenomenon raise the bar as regards the need for cooperation and collaboration among authorities, including across countries. The latter implies that a continuous dialogue should be established with authorities from different digital-related areas, including conduct, data protection or cybersecurity authorities. Finally, regulators and supervisors realize that their knowledge, skills and tools may need to be updated as well.

The road ahead

The efforts of the different bodies to outline the current landscape and start envisaging how this may affect their mandate as regulators and supervisors is much welcomed, as these institutions are a central piece in the new fintech ecosystem. Still, most often their analysis is still at a high level and a lot of work needs to be done to materialise concrete actions. Given the global dimension of most innovations and the increased interconnectedness of the financial system, international cooperation is a must. This is needed in order to define guiding principles at global level that serve to avoid fragmentation across countries' regulatory approaches. The work of the FSB and other international SSBs will be crucial in this endeavour. Also, in this exercise, there are three main areas that deserve deep reflection:

- **The concept and categorisation of the fintech phenomenon.** Most institutions have followed the FSB's definition of FinTech, which is inclusive. However, often they identify fintech firms with smaller new entrants, without encompassing banks or big technological companies. This seems inconsistent with the definition and may lead to an underestimation of the real impact of the phenomenon.

- **The understanding of what is behind a true level playing field**[7], which 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. In relation to this, authorities should further assess the implications of prudential regulation, which often leaves banks in a situation of competitive disadvantage vis-a-vis other players, and work towards eliminating existing loopholes in regulatory frameworks. Also, regulatory sandboxes may be a useful tool to facilitate innovation for all players under safe and equal conditions.

- **The increased role of data as a driver of change.** Data is a key strategic asset in the digital economy, fundamental to reinforce customers' trust and to create compelling value-propositions. Regulators should remain mindful that rules on access and portability of customer data have numerous implications as regards consumer protection, competition and the structure of the financial sector.

7: Urbiola, P. Banks and new digital players: Is there a level playing field? BBVA Research Digital Economy Outlook, September 2017.

6. Artificial Intelligence: a policy approach

Artificial Intelligence is one of the buzzwords of the moment. It is fairly clear that this disruptive technology will noticeably affect the economy and society. Although the exact impact remains to be seen, authorities are trying to understand the potential effects of this technology and devising their initial regulatory strategies.

Artificial Intelligence, the debate

Artificial Intelligence (AI) is defined as the theory and development of computer systems able to perform tasks that normally require human intelligence[8], such as knowledge, representation, reasoning, perception, learning, predicting and interaction with the environment.

AI technology is becoming ubiquitous thanks to improvements in computation and to the wide availability of data, the true raw material for this technology. Moreover, AI seems to be evolving exponentially, and now masters tasks that require strong analytical skills but also shows capabilities that have been traditionally associated with humans, such as creativity[9].

Some experts argue that AI can lead to a Keynesian "life of leisure"[10] by increasing the productivity of factors and reducing the number of dull, dangerous, and dirty activities performed by humans. It could also provide new tools to face global issues such as climate change, food shortage or diseases.

On the other hand, critics believe that an "uncontrolled" adoption of AI could increase unemployment rates, discrimination and social inequality.

Even high-profile personalities such as Elon Musk, Bill Gates, Mark Zuckerberg, Larry Page and Stephen Hawking have engaged in a lively debate on the ethical implications, risks and opportunities of AI.

Policy approaches to AI

In spite of some perceived risks, AI is in most cases just a set of technologies that can be applied to solve a given problem, but it does not entail any special drawback. In those cases, AI should not be regulated differently from other technologies and its adoption should be driven by market forces.

Regarding the applications of AI whose social impact is not neutral, given the global nature of this technology, its assessment should not be undertaken by a country or a region in isolation, but rather be carried out in cooperation with national governments, international organizations and private actors.

8: Schatsky, David, Muraskin, Craig, Gurumurthy, Ragu. 2014. "Demistifying Artificial Intelligence." Deloitte University. November 04, 2014.
9: Last October Google unveiled Alpha Go Zero, an AI system that learnt to play an ancient Chinese board game from scratch and was able to develop innovative play strategies in days.
10: Economic Possibilities for our Grandchildren. John Maynard Keynes.

International organizations such as the UN, the OECD and the WEF have already pointed out the potential risks of this technology and are facilitating the dialogue among international players. At the same time, private partnerships and associations such as the partnership on AI and openAI **are making calls to have ethical issues at the centre of AI developments**.

At a national level, most organizations and governments acknowledge the disruptive potential of AI, but some of them are showing resistance to this technology. This might turn out to be a great mistake, since countries taking a reactive approach could find themselves becoming uncompetitive compared with those leading AI adoption.

Nevertheless, the majority of policymakers are trying to find the right balance between AI promotion and control. There seems to be a consensus also on some topics such as the **ethical concerns** associated with AI, the **potential impact of AI on the economy and the labour market** and the need to **develop new skills related to AI**.

Simultaneously, pioneer regulations are focused mainly on **data privacy and availability, transparency, liability** of AI systems and **the proper functioning of the market** with a significant presence of automated agents. Nevertheless,AI is being tackled at different paces among national governments.

In 2016 the US Artificial Intelligence Task Force, an interagency group promoted by the Obama administration, was arguably the most prolific working group in any administration, producing two papers in October and December 2016 and a strategic plan.

In Europe, the European Parliament issued a report on AI at the end of 2016 and **approved a** resolution **based on this report which recommended the European Commission and the Council to**:

- **submit a Directive on civil laws on robotics**,
- **create a European Agency on robotics**
- **adapt rules on liability** to the specificities of automated systems

Countries such as Canada, China, Japan and South Korea have established AI strategies which share some common features:

- They intend to become world leaders in AI deployment,
- making use of similar tools: cooperation, education, support (either legal or financial) and research.

As part of these first movements, **some countries/organizations have already allocated funds to develop AI**, although with disparate amounts of funding and objectives. For instance, South Korea and the European Union have assigned almost US$1 billion to public-private partnerships, while Canada and the UK have allocated US$100 million and US$20 millionrespectively to further investment and research.

Regulation of AI in Financial Services

Regarding the financial sector, controls on robo-advisors and automated trading systems are spearheading the financial regulatory framework.

In particular, the SEC issued some guidance on robo-advisors in February 2017 and the UK is actively giving guidance on robo-advice through the FCA's Advice Unit. The two authorities are optimistic on the potential of robo-advice but underline the need to ensure customer protection and transparency.

As for automated trading, the Futures Commission of Hong Kong published a circular in December 2016 pointing out areas for improvement in algorithmic trading, mainly asking for enhanced controls and more formalization of some processes.

The European Supervisory Authorities ran a consultation on the use of Big Data by Financial Institutions during the first quarter of 2017 and the EBA published a report on innovative uses of data in June 2017. The main conclusion was that no specific action from financial authorities is needed at this moment.

Artificial Intelligence was also part of the consultations on FinTech launched by the European Commission, EBA and BCBS during the year. In those consultations, authorities requested opinions on the need for specific approaches to AI in finance.

Moreover, it is felt that open banking initiatives such as the UK Open Banking Standard and the revised EU Payment Services Directive (PSD2), which allow third parties to access data of customers' accounts, in combination with more far-reaching regulations such as the EU General Data Protection Regulation (GDPR) could facilitate access to and sharing of financial data. This will expand the data sources available to develop AI systems and, consequently, the rate of adoption of this technology by the financial sector.

Finally, on 1 November 2017 the Financial Stability Board published a paper on the impact of AI and Machine Learning on financial services which brings AI into the spotlight of financial stability policies.

In conclusion, although Artificial Intelligence is still a nascent technology, its wide availability and growing adoption by companies, financial institutions and public authorities make an assessment of its future social and economic impact necessary. This assessment should be undertaken in cooperation among national governments, international organizations and private actors.

Nevertheless, governments should devise their own AI strategies to become familiar with the challenges that this new technology poses and support the development of AI within their borders so that they are well positioned to compete internationally if AI becomes a widely adopted technology as is expected.

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.

The content of this document is protected by intellectual property laws. It is forbidden its reproduction, transformation, distribution, public communication, making available, extraction, reuse, forwarding or use of any nature by any means or process, except in cases where it is legally permitted or expressly authorized by BBVA.

BBVA | Research

This report has been produced by the Digital Regulation Unit:

Chief Economist for Digital Regulation Unit
Álvaro Martín
alvaro.martin@bbva.com
+ 34 91 537 36 75

María Álvarez
maria.alvarez.caro@bbva.com

Edward Corcoran
edward.corcoran@bbva.com

Jesús Lozano
jesus.lozano@bbva.com

Lucía Pacheco
lucia.pacheco@bbva.com

Alicia Sánchez
alicia.sanchezs@bbva.com

Javier Sebastián
jsebastian@bbva.com

Ana Isabel Segovia
ana.segovia@bbva.com

Pablo Urbiola
pablo.urbiola@bbva.com

With the contribution of:
Cristina Plata
cristinateresa.plata@bbva.com

BBVA Research

Group Chief Economist
Jorge Sicilia Serrano

Macroeconomic Analysis
Rafael Doménech
r.domenech@bbva.com

Global Macroeconomic Scenarios
Miguel Jiménez
mjimenezg@bbva.com

Global Financial Markets
Sonsoles Castillo
s.castillo@bbva.com

Global Modelling & Long Term Analysis
Julián Cubero
juan.cubero@bbva.com

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

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

Countries Coordination
Olga Cerqueira
olga.gouveia@bbva.com

Digital Regulation
Álvaro Martín
alvaro.martin@bbva.com

Regulation
María Abascal
maria.abascal@bbva.com

Financial Systems
Ana Rubio
arubiog@bbva.com

Financial Inclusion
David Tuesta
david.tuesta@bbva.com

Spain & Portugal
Miguel Cardoso
miguel.cardoso@bbva.com

United States of America
Nathaniel Karp
Nathaniel.Karp@bbva.com

Mexico
Carlos Serrano
carlos.serranoh@bbva.com

Turkey, China & Geopolitics
Álvaro Ortiz
alvaro.ortiz@bbva.com

Turkey
Álvaro Ortiz
alvaro.ortiz@bbva.com

China
Le Xia
le.xia@bbva.com

South America
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

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