BBVA | RESEARCH

Digital Economy Outlook

JANUARY 2017 | DIGITAL REGULATION UNIT

Index

Summary

Algorithms challenge the banking industry

Algorithms are at the core of data analytics, the foundation on which data-driven societies are built. The digital transformation of the economy and the development of new platform ecosystems also rely heavily on them. A successful application of algorithms requires ethics and transparency to become key considerations in their design. Besides, providing appropriate protection for algorithms is essential for the well functioning of the financial services industry, as they are increasingly becoming a competitive asset for banks.

Does blockchain fit into current legal frameworks?

The decentralized nature of blockchains can imply some legal uncertainties. Blockchain, as a technology, cannot be regulated: only activities performed using the technology can. However, there are a number of transversal regulatory challenges that, regardless of the specific use case, are going to be present and that will have to be addressed to ease its adoption.

Turning the spotlight on shadow banking: pros and cons of the darkness

Non-banking entities and activities, such as crowd-funding and peer-to-peer lending, can be a helpful complement to the banking sector to support investment and economic growth. However, they can also be a source of systemic risk if not properly supervised and regulated. Therefore, an adequate balance is needed to maximise the benefits while at the same time minimising the gloomy consequences of financial instability and regulatory arbitrage.

The Internet of Things and digital banking

The increase in the number of connected devices will make the Internet of Things a key source of information for knowing our banking customers better. The use of this technology will also allow to attract generations of consumers who are get used to digital media, allowing them to contract to banking products without the need to be physically present in the branch, as well as offering them a more complete user experience, with greater control over their personal finances.

1. Algorithms challenge the banking industry

Algorithms become a competitive asset for banks, demanding stronger ways of protection to foster innovation

Algorithms are at the core of data analytics, the foundation on which forward thinking societies are built. The digital transformation of the economy and the development of new platform ecosystems also rely heavily on them. Data-driven organizations, such as financial institutions, require appropriate and stronger ways of protecting algorithms, as they are part of the organizations know how. Besides, ethics and transparency become key considerations in their design.

Abstract

In the financial services industry, algorithms are intensively used for various purposes, from offering more personalised finance products due to data analytics based in algorithms to improving areas like investment analysis, risk assessment, fraud prevention or trading. The overall goal of the use of algorithms is to extract value from data, for the benefit of both consumers and organizations. Algorithms, as a competitive asset for banks, need stronger ways of protection to drive value creation and foster innovation for the delivery of new products, services and processes. Avoiding discrimination and transparency on the use of algorithms also becomes a must for banks. The new General Data Protection Regulation (GDPR) is a relevant rule that promotes transparency while reinforces the rights of individuals in relation to data protection and automated decision making.

Know how protection to foster innovation

Algorithms allow for higher quality services as well as better decision making, for the benefit of both consumers and enterprises. For this reason, the legal framework under which algorithms operate should not limit their innovative potential but reinforce it. Algorithms protection becomes essential for all data driven organizations, while maximizing the economic value of an algorithmic asset critically depends on understanding the nature of the intellectual property rights involved and how best to use the available forms of protection.

As for the way to legally protect algorithms, there is no copyright or industrial property law explicitly referred to algorithm protection. Moreover, algorithm protection varies depending on the jurisdiction. There are several mechanisms of protection to be considered: patents, copyright, know how protection or industrial secrecy.

There has been much debate as to whether algorithms and computer programs are more like processes and machines, therefore eligible for patenting, or more like the laws of nature, therefore unpatentable[1]. On the other hand, patents are two-edge swords, as they confer market power on their holder and therefore limit competition. Software patents have traditionally been questioned[2]. In the EU, as for the protection through patents, there is an explicit exclusion of mathematical methods, as long as these methods are the unique

1: Maier, Gregory J.: "Software protection-integrating patent, copyright and trade secret law", *Journal of the Patent and Trademark Office Society*, vol.69, nº3, pag. 152-165,1987.
2: Study of the effects of algorithmic patent claims for computer implemented inventions, commissioned by DG Information Society of the European Commission, June 2008.

purpose of the patent[3], but this instrument can be used if the algorithm is integrated into another invention or if it is part of it. As for copyright protection, it protects the expression of ideas, methods or theories in a written work or as software. One of the important advantages of patents over copyright is that patents protect against independent developments, while copyright only protect against derivation from protected works. Therefore, a copyright applied to software would appear to protect only the intellectual property embodied in software as a mode of expression.

Many enterprises protect algorithms through industrial secrecy and know how protection. On June 2016, the Directive 2016/943 on the protection of undisclosed *know how* and business information (trade secrets) against their unlawful acquisition, use and disclosure, was adopted. As long as the algorithm has a commercial value and has been kept secret with specific measures, this Directive would offer protection against an unlawful access or disclosure and offers ways to obtain compensation for damages. This Directive is a step forward for businesses to protect their innovative work and preserve competitive gains.

Discrimination risk and supervision

An algorithm is a collection of instructions for carrying out a task, where certain inputs are transformed into outputs. They can be defined as "a mathematical method to solve a problem that consists of exactly defined instructions"[4]. Algorithms can also be defined as "a formally specified sequence of logical operations that provides step-by-step instructions for computers to act on data and, thus, automated decisions"[5]. Algorithms are helpful for both consumers and organizations but demand a proper design and monitoring. Alongside their potential benefits, big data technologies can be used to discriminate against individuals, potentially enabling discriminating outcomes, reducing opportunities and choices available to them. Therefore, there is a "need to ensure fairness in automated decisions, preserving constitutional principles, enhancing individual control over personal information, and protecting people from inaccurate data"[6]. So-called *black box* algorithms cannot guarantee such fairness, as they are basically systems in which the inner workings are mysterious, where we can observe their inputs and outputs but we cannot infer how one becomes the other[7].

In order to ensure an appropriate knowledge of how algorithms actually work, Mayer-Schönberger & Cukier (2013)[8] discuss the possibility of introducing the role of *algorithms monitors*, scientists who audit algorithms. The creation of professional bodies of algorithm monitors could be considered, with members, just like doctors, lawyers, architects and other professions, who are subject to strict conduct and ethical codes in their activities. Another idea would be to establish internal algorithm monitors within organizations to monitor *in situ* the activities being conducted with personal data, protecting in particular the interests of people who might be affected. There would be an algorithm *ombudsman* to make sure that the entire data handling process, from the moment data is obtained, up to the final outputs, is managed using ethical and scientific good practice.[9]

3: Art.52 European Patent Convention.
4: Futscher, Gerarld: *Algorithmic thinking: the key for understanding computer science*, Vienna University of Technology, Institute of Software, Technology and Interactive systems, 2006.
5: Solon Barocas et al: Data & civil rights: technology primer (2014). http://www.datacivilrights.org/pubs/2014-1030/Technology.pdf [https://perma.cc/X3YX-XHNA].
6: *Big Data: Seizing opportunities, preserving values*, White House, February, 2015, p.6.
7: Pasquale, F:"The black box society: the secret algorithms that control money and information", Harvard University Press, 2015.
8: Mayer-Schönberger, Viktor & Cukier, Kenneth: *Big Data: A revolution that will transform how we live, work and think,* Houghton Miffin Harcourt, 2013.
9: Alonso, J., Tuesta, D., Cuesta, C., and Fernandez de Lis, S.: "An approach to the economy of personal data and its regulation", Economic Watch, BBVA Research, Sept. 2014.

Algorithms also pose risks in relation to possible market distortion, collusion prices or herd behaviour risk among industry players. Regulators are beginning to grasp the implications of these powerful tools, finding ways to prevent collusion among machines. It is a relevant challenge Competition law enforcers will face[10].

GDPR and the 'right to explanation': algorithm transparency

The General Data Protection Regulation (GDPR)[11] is an ambitious regulation in the field of data protection that will be applicable from May 2018 in the European Union. As regards automated decision making (including profiling) that significantly impact data subjects, it reinforces a right to explanation of the logic of algorithms. Opacity is at the very heart of new concerns about algorithms[12]. To address it, probably widespread educational efforts would make consumers more aware about the mechanics of algorithms. "Transparency is not just an end in itself, but an interim step on the road to intelligibility"[13]. Beyond the right to obtain human intervention, to obtain an explanation of the logic and consequences of algorithms, a data subject's right to express his or her point of view and to challenge the decision, the Regulation does not specify the type of measures to be taken. What does it mean and what is required to explain an algorithmic decision? The answer to the question is not obvious. The GDPR implies a challenge for all industries, and especially for financial services firms, as data scientists will have to design efficient algorithms that can be explained in an understandable manner, striking the right balance between transparency and know how protection, avoiding a full algorithm disclosure.

Conclusion

Algorithms are fundamental elements not only for the banking industry but for all industries that are data-driven and rely on an intensive use of automated processing. Algorithms are part of the organizations' *know how* and demand stronger ways of protection. However, any enterprise that processes personal data from European residents, offering goods or services to them, has to be able to explain the logic of algorithms in automated decision making, including profiling. The GDPR is challenging data scientists, on the one hand, who must design efficient algorithms that can be easily explained and avoid discrimination, while it is also challenging the entire organization to build a strategy for a strong algorithm protection framework.

10: "*Policing the digital cartels: price-setting algorithms mean regulators must now tackle collusion among machines*", January 8th 2017, Financial Times
11: General Data Protection Regulation (679/2016).
12: Burrell, Jenna: "How the machine 'thinks': understanding opacity in machine learning algorithms", *Big Data & Society*, SAGE Journals, January 2016.
13: Pasquale, F.: *op, cit,* pag. 8.

2. Does blockchain fit into current legal frameworks?

The decentralized nature of blockchains can imply some legal uncertainties

Blockchain, as a technology, cannot be regulated: only activities performed using the technology can. However, there are a number of transversal regulatory challenges that, regardless of the specific use case, are going to be present and that will have to be addressed to ease its adoption.

Main regulatory challenges facing blockchain

The immaturity of blockchain-based initiatives and the piloting phase of identified use cases means that specific **regulation of blockchain activities in the financial services industry is still non-existent**. Some current regulations will apply to blockchain-based services: for instance, smart contracts on the blockchain will at least have to comply with regulation on contracts applicable in every jurisdiction. Then, depending on the financial services offered on the blockchain (payments, lending, investment, etc.), regulation will have to be applied to these services. However, when looking at the big picture in blockchain, there are a number of **broad regulatory challenges** that will have to be addressed at some point in the future.

A more detailed analysis of these challenges can be found in BBVA Research's Working Paper "Blockchain in Financial Services: Regulatory landscape and future challenges for its commercial application."

1. **Inclusion of payments and international transfers service providers using blockchain technologies in KYC, AML / CFT regulations** in order to ensure a level playing field and control potential illicit uses of cryptocurrencies. Exchange platforms and custodian wallet providers were already proposed for inclusion in the 4th European AML Directive on July 2016.
2. **Legal framework regarding the nature of blockchains and distributed ledgers.** Distributed ledgers are not tied to a specific location. In terms of jurisdiction and applicable law, territoriality is an issue because every node of the network may be subject to different law, and there is no "central party" whose nationality could serve as an "anchor" for regulation. Similarly, liability is also a concern, because there may not be a party who is ultimately responsible for the functioning of the ledger. Nevertheless, in the case of "federated" ledgers it would depend on whether the ledger itself had any kind of underlying legal entity or not.
3. **Legal framework for the recognition of blockchains as single sources of truth.** Although there is wide consensus about the immutability of information in a well-defined blockchain, there is still a lack of legal recognition of this immutability, preventing it from being used so far as an argument in front of any courtroom yet. A related issue is the storage of identity information in a blockchain. The use of blockchains as "single sources of trusted identity" is the ultimate goal of many players and a definitive step towards a "universal digital identity", but the recognition of blockchains as immutable sources of truth is a pre-requisite.

4. **Regulation on how the "right to be forgotten" shall be interpreted.** The immutability of the blockchain might collide with the "right to be forgotten" recognized by some data protection regulations, as it is the case in Europe [14]. A potential solution to reconcile both could be to substitute "deletion" by "impossibility of use" of personal information by third parties. This could be achieved with automatic encryption of information when certain conditions are met (a smart contract could be involved) or alternative solutions to prevent access to that information.
5. **Legal framework on the validity of documents stored in the blockchain as a proof of possession or existence.** On top of the recognition of the blockchain as a single source of truth, there is a second level of recognition needed for certain businesses: that a document stored in the blockchain representing the ownership or existence of an asset really proves such ownership or existence. If the process of verifying the veracity of the document prior to its inclusion in the blockchain were robust enough, the recognition of the blockchain as an immutable source of trust would imply recognition of the document as proof of existence or ownership. Again, there is no court in the world accepting this yet.
6. **Legal framework on the validity of financial instruments issued on the blockchain.** When using the blockchain as a platform to define "native" financial instruments, such as bonds or derivatives, the recognition of the legal validity of these financial instruments by the corresponding regulators and supervisors is needed. The ultimate case would be, of course, money. Native money issued on a blockchain could have a huge impact that goes beyond the limits of this article.
7. **Legal framework for smart contracts.** Territoriality and liability issues are also applicable to smart contracts. Regarding jurisdiction, not only does the ledger itself has no specific location, but contracting parties can be subject to different laws in their countries as well. Regarding liabilities, multiple parties may be involved in smart contracts: the contracting parties, the contract creator (usually a coder) and a contract custodian. Apart from the obvious possibility of contracting parties not fulfilling the contract, there is a chance of the contract itself working badly, because of mistakes in coding or defects in design: who would be liable in that case?
8. **Legal framework for information in blockchains from the perspective of cross-border flow of data and data protection.** The distributed shared nature of blockchains has direct implications on stored data. Although in public blockchains information is accessible to all the nodes of the network, in "federated" ledgers the "slices" of information accessible to each participant must be carefully managed. Also, as already mentioned, there is also a territoriality issue that affects data. Information in the ledger is decentralized so there is an inherent cross-border data flow that may violate existing regulations.
9. **Legal framework regarding the use of the blockchain as a valid ruling register for the Internet of Things (IoT).** Since in the IoT realm everything has an identity, it would be useful to have a common shared register to store things' "identity" and information, and to allow transactions between them. This idea of one or many interrelated "director ledgers" for the IoT is barely nascent and will not be operational in the short term. However, it will require a legal framework in which these director ledgers are recognized as valid ruling registers for the IoT. All the previously mentioned issues of territoriality, liability and enforceability of smart contracts are of course applicable to this case.

14: Any European citizen has the right to have their personal information deleted from second parties' electronic or paper records or databases.

10. **Definition of regulatory reporting standards on the blockchain.** Recent research about RegTech[15] shows that blockchains can be useful tools in this field. Having all the transaction information in a shared ledger in almost real time could allow regulators/supervisors to monitor financial activity without waiting for required reports from financial institutions. However, standards are needed on the kind and format of transaction data that have to be stored in the ledger(s) so regulators can easily extract the information. And, most importantly, data to which each regulator/supervisor should have access to must be clearly defined.

11. **Definition of regulatory sandboxes**[16] in order to test these technologies, including criteria for blockchain projects to enter the sandbox, limit of scale of the activities carried out within the sandbox, authorisation process rules and requirements, waivers or modifications to particular rules if testing activities would breach them, alignment of the sandbox rules to current legislation, and proper consumer safeguards.

Conclusion

Blockchain technology is being increasingly considered as a potential game-changer for financial services. However, to take the next step towards its commercial development, there are legal uncertainties that must be clarified. Some of these uncertainties have to do with fundamental concepts of law, and imply the need for a deep reflection about the meaning of some established ideas in a decentralized digital world.

15: Technologies applied to the addressing of regulatory requirements.
16: Controlled environments in which firms can test innovative solutions with real customers without immediately incurring the entire normal regulatory burden.

3. Turning the spotlight on shadow banking

Pros and cons of the darkness

Non-banking entities and activities, such as crowd-funding and peer-to-peer lending, can be a helpful complement to the banking sector to support investment and economic growth. However, they can also be a source of systemic risk if not properly supervised and regulated. Therefore, an adequate balance is needed to maximise the benefits while at the same time minimising the gloomy consequences of financial instability and regulatory arbitrage.

Light on the shadow

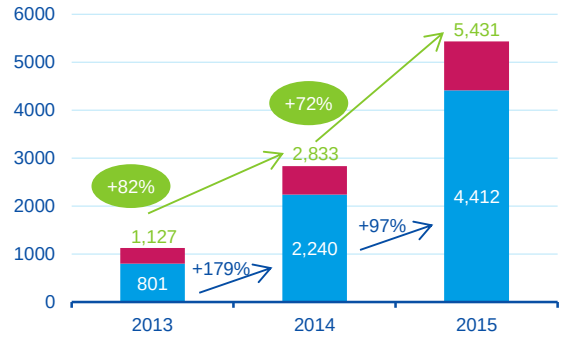
The concept and the metrics for shadow banking are still pending. Shadow banking is generally defined as "credit intermediation that involves entities and activities fully or partially outside the regular banking system"[17]. In 2015, the Financial Stability Board (FSB) proposed a more accurate definition considering five economic functions and their contributions to financial stability risks[18]. In addition to that, a group of economists from the International Monetary Fund (IMF) proposed an alternative definition based on the sources of funding and whether or not they are "non-core liabilities[19]. They consider that the previous definitions are short-sighted because they "miss significant non-traditional banking activities carried out by banks themselves, thus leading to an incomplete picture of [shadow banking] and of the potential vulnerabilities associated with it".

The FSB estimated that non-bank financial intermediation totalled EUR 102.2 trillion[20] at the end of 2014 (40% of total financial system assets) and EUR 29.6 thousand billion using the narrow definition. **In the EU, at the end of 2015**, the European Systemic Risk Board (ESRB) calculated EUR 37 million trillion[21] in terms of total assets (36% of total EU financial sector assets) using the broad definition. **Focusing on the online sector, by the end of 2015**, the total for alternative finance in the Asia-Pacific region was approximately EUR 95.6 billion, EUR 33.6 billion for the Americas, and EUR 5.4 billion (+92% YoY) in Europe. The data show that the European market is still small when compared to the other two regions. In Europe, the United Kingdom is the largest market by a considerable margin[22].

17: Source: ESRB. EU Shadow Banking Monitor No 1 / July 2016 Page 6.
18: Source: *A measure of shadow banking based on economic functions* (sect.2.) FSB 2015 Global Shadow Banking Monitoring Report.
19: Core liabilities are issued only by banks and non-core liabilities can be issued by banks, money market funds and other financial intermediaries. Explanation can be found in *Shedding Light on Shadow Banking* Artak Harutyunyan et al. IMF WP. Jan 2016.
20: 10^12. Source: FSB's 2015 Global Shadow Banking Monitoring Report for more. Exchange rates 1.21410 USD/EUR. Source: BCBS.
21: 10^18
22: Source: Sustaining momentum: the 2ndEuropean alternative finance industry report. University of Cambridge & KPMG. 2016

Figure 1

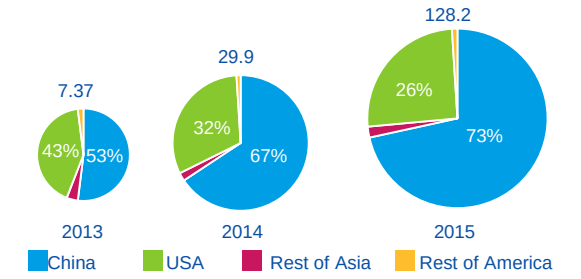
European Online Alternative Finance Market Volumes 2013-2015 (in EUR million)



Source: BBVA Research based on University of Cambridge & KPMG

Figure 2

Asia-America Online Alternative Finance Market Volumes 2013-2015 (in EUR billion)



Source: BBVA Research based on University of Cambridge & KPMG

Digital shadow banking

With the emergence of new technologies, digital finance platforms have expanded rapidly. **They facilitate millions of transactions every day for individuals and businesses** and play a significant role in the provision of a viable 'alternative' to traditional sources of financing. A variety of online platform-based models exist, such as donation-, reward- and equity-based crowd-funding, peer-to-peer consumer and business lending, invoice trading and debt-based securities.

In Europe, funding for businesses has increased considerably since 2014, becoming an important source of finance for entrepreneurs, start-ups and small & medium-sized enterprises (SMEs). In 2015, EUR 536 million of business finance was raised through online alternative funding models, providing capital to 9,442 businesses. It is providing early stage investments to start-ups and growth capital to SMEs, stimulating regional economies and funding worthwhile causes. It should also be noted that, according to the European Commission, in recent years, access to financing has become overall the least important problem for SMEs, while in 2009 it was the second most urgent one. **The alternative business funding market has probably been a relevant variable in explaining that improvement.**

At this point, we would like to highlight that one of the largest lending platforms is applying for a banking licence in the UK. It will become the first *P2P banking company* under the scrutiny of the Financial Conduct and Prudential Regulation Authorities. Business diversification, synergies and consumer protection seem to be the main drivers of that strategy: deposits raised from the bank would fund P2P loans. Last, but not least, the platform will also bring protection for its consumers' deposits, given the fact that they will be included under the umbrella of the Financial Compensation Scheme, not extended to "pure" P2P depositors.

There are different possible explanations for the increase in alternative business funding platforms, one of them being the **financial crisis**: with near-zero interest rates, as investors entered these new markets, searching for the higher rates available due to P2P assets exposure. For potential borrowers, there is a wider range of credit options, as regulation has become stricter and a lack of trust in the traditional banks has expanded. Another reason that explains the expansion of alternative finance could be linked to the **nature of the traditional banking market**, where high entry barriers make it difficult for new banks to

emerge. Financial intermediary costs have remained stable for years, while **the new online lender players face lower costs due to their lack of branches and lower administrative burden.**

Yet another possible explanation for this boom could be that finally **digitisation is mature enough in society** for the public to use on-line channels to perform financial transactions. But the most important driver is probably the **rise of new technologies**, which has enabled the rapid entry of new players into the financial markets.

Digital Regulation

As a result of the expansion of the alternative finance market, governments **have started to issue local regulations with different approaches**, ranging from more restrictive ones in countries such as the US, Germany or France, versus less restraining norms in the UK and New Zealand.

In Europe, **the lack of a common legal framework may be hampering the development of online-based platforms,** as it implies major risks to both consumers and investors and does not ensure a level playing field between financial and non-financial institutions.

Recently, **fraud incidents regarding crowd-funding platforms have proved that some regulation is needed for these entities**. One of the most significant cases is related to the biggest Chinese P2P lending platform Ezu Bao, which collected 50 billion Yuan ($7.6 billion) in less than two years. Investigations revealed that top executives used investors' money to enrich themselves. After this, China issued a regulation to toughen its control of peer-to-peer lending companies.

Some of these new entrants (Lending Club, Prosper, Kabbage) favour the use of other terms, such as "market-based financing", instead of "shadow banking" to define their business. In any case, issues such as **insufficient understanding on the part of consumers, the collapse of platforms, loan defaults, cyber-attacks and credit and/or investment protection must be addressed by the authorities in regard to these players**; regulation is therefore becoming another key driver for the adoption of these alternative finance solutions.

Conclusions

Shadow banking can be a useful tool for helping the banking sector in the provision of credit, especially in Europe, where approximately two-thirds of funding depends on banks[23]. Non-banking funding can also contribute to facilitating market liquidity and risk sharing and to fostering competition and innovation through the support of new ideas and projects. In particular, digital-based platforms have grown dramatically in size and scale over the past few years. On the other hand, if not adequately supervised and regulated, non-bank funding can contribute to an increase in systemic risk through interconnections with a few players from the financial system, especially the banking sector. Besides, non-bank funding might weaken the level-playing-field as a consequence of regulatory arbitrage due to undeserved advantages. The setbacks relating to fraud and cyber security attacks suffered by some P2P need to be addressed by the regulators, providing a comprehensive framework for the development of these shadow banking activities, and allowing the development of instruments that can contribute to maximizing the advantages of digital shadow banking while minimizing its inconveniences. Consumers could take advantage of gains in efficiency and have access to wider and more competitive services and, last but not least, financial entities would have the possibility of bolstering their innovation projects and learning faster.

23: Source: ECB "Shadow banking in the euro area: risks and vulnerabilities in the investment fund sector" No 174. July 16. Point 2.2

4. The Internet of Things and digital banking

The increase in the number of connected devices will make the Internet of Things a key source of information for knowing our banking customers better

The use of this technology will also allow to attract generations of consumers who are get used to digital media, allowing them to contract to banking products without the need to be physically present in the branch, as well as offering them a more complete user experience, with greater control over their personal finances.

Banks react to a new ground-breaking panorama

The Internet of Things (IoT) is a potentially disruptive technology, which reconsiders the use of traditional products and processes in a wide range of industrial sectors. According to the *International Telecommunications Union* (ITU), the IoT is defined as a worldwide infrastructure for the information society allowing access to advanced services by means of the physical and virtual interconnection of things, based on existing and evolving interoperable information and communication technologies[24]. In mid-2015, TATA Consulting Services published the results of a survey which included the IoT expenditure budgets for 13 industrial sectors. According to this study, the telecommunications sector was expected to reach the highest IoT expenditure in 2018 (US$169 million), followed by the **finance and banking sector** (US$153 million) and the manufacturing industry (US$136 million). This highlights the banking sector's reaction to the possible disruption posed by an emerging technology.

McKinsey Global Institute[25] estimates a potential annual economic impact (gross value added) of between USD US$2.7 billion and US$6.2 billion[26] by 2025, mainly as a result of savings in costs and increased productivity due to the use of this new technology. For example, the logistics operator UPS has stated that its productivity has increased through better monitoring of its delivery trucks and delivery team. According to their figures, “a typical driver can normally deliver 90 packages a day, and thanks to the optimisation of our process, it has now increased to 120”[27]. Secondly, by the generation of revenue through new products and processes. For example, the technology firm OnStar now uses an automatic replacement system in the event of accident, monitoring of stolen vehicles and roadside assistance, among other services.

Attracting, understanding and retaining customers

For the banking sector, improvements in terms of productivity and costs savings will presumably be the result of **digital onboarding** (the process through which a relationship with a new consumer begins through digital channels) through devices which are able to identify a customer through their biometric data and the use of

24: *The Internet of things — Machines, businesses, people, everything*, ITU News, 2013.
25: Manyika, Michael Chuim et al, *Disruptive Technologies: Advances that will transform life, business, and the global economy*, McKinsey Global Institute, 2013.
26: Based on Spanish figures.
27: *The Internet of Things: Making sense of the next mega-trend*, Goldman Sachs, 2014.

smartglasses, for example; as well as improvements to intelligent buildings, in which energy efficiency will improve thanks to greater automation and connectivity.

Meanwhile, a possible strategy for increasing revenue stream is that of attracting new customers (with a special focus on **millennials** and the **Generation Z**), ensuring a greater knowledge and understanding of them and retaining their business.

Banks have an important competitive advantage in terms of their new customers, as they hold a great deal of information on the consumer patterns and behaviour of users. The difficulty lies in attracting these new customers and retaining them over time, given the highly competitive FinTech environment and the trend toward people having greater control and empowerment over their personal information.

How therefore can banks attract the new generations of consumers and keep them, ensuring customer loyalty? Firstly, by getting to know the customer. Each generation, and in particular the millennials, do not follow the same behavioural patterns that are identical to their predecessors. The **user experience** plays a much more important role in this journey, with some banks succeeding in finding ways to catch the attention of future customers, who may well find themselves in a cash free world. An example of such a bank is New Zealand's ASB. In 2015, it launched an electronic toy in the form of an elephant (*Clever Kash*) which becomes a virtual money box. Children receive money directly from their parents' bank accounts which is paid into their accounts. The toy allows interaction with the mobile app, ensuring that the child learns savings awareness.

Secondly, the new generations of customers are connected to their smartphones, meaning that the banking sector has a key role to play in the digital interaction of users. A good example here would be the role played as **payment managers**. There are numerous applications that make payments via a mobile phone, although future payments will not only involve a connected phone but also cars capable of automatically paying for fuel and smart fridges, as well as other objects.

Finally there is a business stream that focuses on **data exploitation**. Thanks to the endless torrent of data sent from IoT devices, information can be obtained in real time through advanced analytics, which are implemented either through the banks themselves or the transfer of non-personal data to third parties. BBVA has an application based on Big Data (*Commerce 360*) which offers commercial intelligence to small businesses[28]. The data stored regarding the behaviour of a certain individual represents a commercial advantage in itself, where the user has given their consent and all relevant data protection legislation and guarantees are fully complied with, as it may have considerable value to third parties. If the consumer in question authorises the use of their personal data (including data stemming from IoT-connected devices), companies will be able to use this information to microsegment the consumer mass, offering not only products that are closer to consumer tastes, but which are also affordable.

Nevertheless, IoT in the banking sector has certain difficulties to overcome in terms of implementation. Firstly, cybersecurity severely limits movements in the sector, as was seen after the DDoS (Distributed

28: BBVA.com, (9 August 2016), Commerce 360, data offering new opportunites for your business, URL: https://www.bbva.com/es/noticias/economia/macroeconomia/commerce-360-datos-abren-nuevas-oportunidades-negocio/

Denial-of-Service) in October 2016[29], when IoT devices were shown to be lacking in terms of having effective security standards in place. Furthermore, such devices do not receive security patches and updates. There is also a problem when it comes to data ownership attributing responsibilities regarding its use. In many cases, people are questioning such ownership lies with the user or the company supplying or managing the device. There has also been criticism as to whether the data thus gathered may result in price discrimination. As was mentioned previously, a greater awareness of user behaviour patterns allows microsegmentation based on purchasing power. This makes it possible to ensure that certain profiles are automatically excluded from specific market segments on the basis of the information provided previously. Similarly, some companies will be able to take advantage of the available information in order to push up the price of products to customers with higher purchasing power. This will result in a lively debate which will need to be closely followed in coming years.

29: Guillén, B, Faus, J, Jiménez Cano, R, (22 October 2016), Mass cyberattacks bring down the websites of large companies, *El País*. URL: http://tecnologia.elpais.com/tecnologia/2016/10/21/actualidad/1477059125_058324.html

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

María Álvarez
Maria.alvarez.caro@bbva.com

Vanesa Casadas
vanesa.casadas@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

Javier Anatole Pallás Gozálvez
javieranatole.pallas@bbva.com

With the contribution of:

Arturo Fraile
arturo.fraile@bbva.com

Álvaro Romero
Alvaro.romero.mateu@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