BBVA | RESEARCH

Nº 16/20
December 2016

WORKING PAPER

Blockchain in financial services: Regulatory landscape and future challenges for its commercial application

JAVIER SEBASTIAN CERMEÑO

Blockchain in financial services: Regulatory landscape and future challenges for its commercial application

Javier Sebastian Cermeño

December 2016

Abstract

How are distributed ledger technologies impacting the regulatory framework?

Distributed ledger technologies (DLTs), including blockchains, are increasingly getting a massive interest from established industries. The interest is especially strong among financial services firms, which are starting to see DLTs as a potential driver of huge savings in infrastructure and back-office processes. Besides, DLTs might become a facilitator for the development of new digital businesses leading to new sources of revenue. However, DLTs are still far from being ready for mass adoption, due to some unsolved challenges on the technological, operational, business and regulatory sides.

Keywords: Regulation, Virtual Currencies, Distributed Ledgers, Blockchain

JEL classification: K24 (Cyber Law), O33 (Technological Change: Choices and Consequences • Diffusion Processes)

Introduction

Blockchain technologies have being heralded as the next big disruption in financial services. Potential uses may indeed bring huge benefits to the industry and give birth to a whole new generation of services. However, a lot of legal uncertainties which have to be solved to facilitate the mass adoption of these technologies still surround the field. The aim of this paper is to depict the current regulatory landscape regarding blockchain and to identify the main challenges to be addressed in this context.

In the first section of the paper, basic concepts are reviewed to give the reader a foundational understanding about the singular characteristics of blockchain technologies. The second section describes the current state of blockchain regulation in relevant geographies around the world. The third section is dedicated to a reflection about the use of blockchain as a potential tool for regulators themselves. The fourth section identifies and briefly analyzes the main regulatory challenges to be addressed. A fifth section is dedicated to other technological and operational challenges associated to blockchain, not directly related to regulation but that could eventually derive in new regulatory needs. Finally, a conclusion summarizes the findings in the document.

Some details about public declarations from regulatory authorities' representatives have been displaced to the annexes in order to give additional information about the regulators' mindset in cases where actual regulations have not been formulated yet.

1. Review of basic concepts

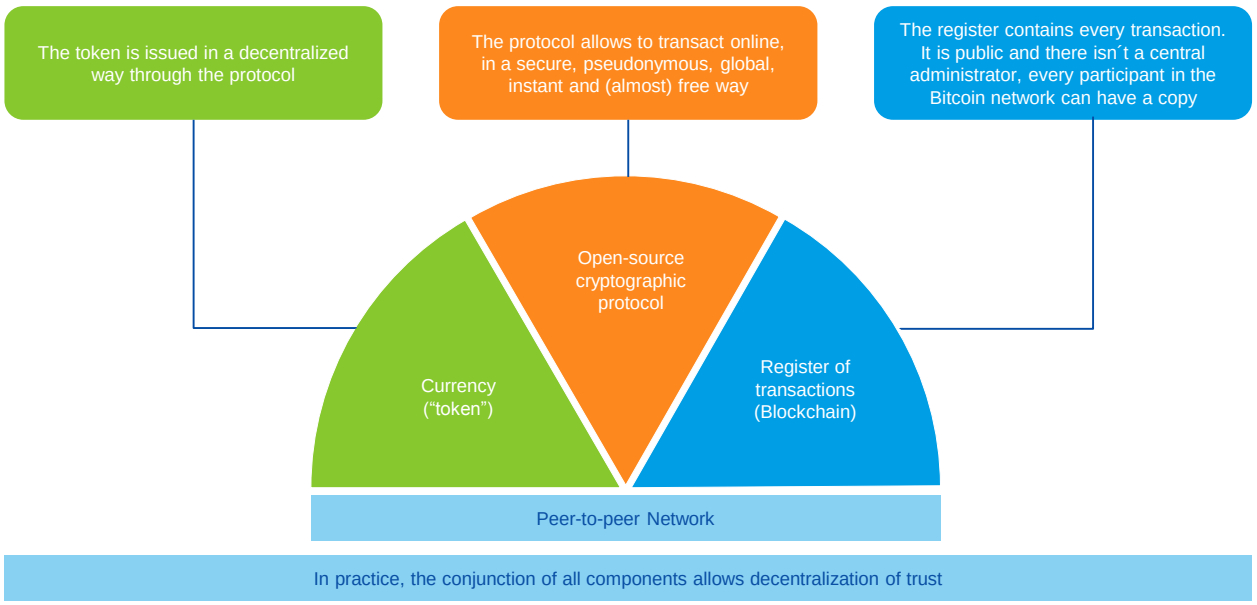
The origin of this wave of interest around distributed ledger technologies (DLTs) comes from the concept of blockchain which appeared as a building block of the first defined cryptocurrency scheme, Bitcoin, and has been upgraded to a more general category of technologies, the distributed ledgers.

Although both names are often used interchangeably, they are not strictly the same. In short, the purest blockchain entails a public network and a "mining" process based on a proof-of-work (PoW) consensus mechanism in which tokens are issued in a decentralized way, while distributed ledgers can be public, federated or private, and don't necessarily entail a PoW consensus mechanism or even a "mining" process. In fact, token issuance can be centralized while the ledger is decentralized.

From its inception, Bitcoin was defined primarily as a set of four components, of which tokens (or 'coins') are only one of them, as we can see in figure 1.

Figure 1

Bitcoin is a set of four components



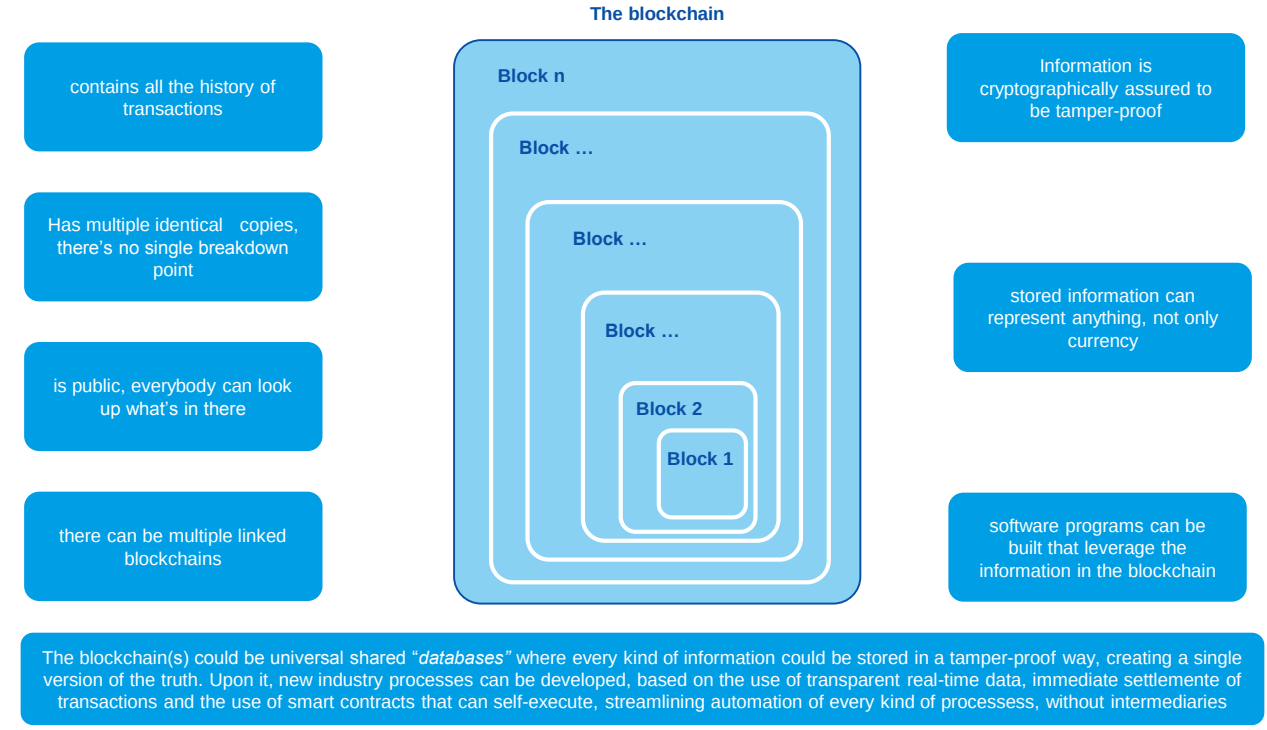
Source: BBVA Research

Although in a first moment all the attention was drawn to the currency (or "token" piece, the bitcoin currency) the evolution of disruptive thought about cryptocurrencies in general has led to a more intense interest on the underlying technology: the open-source cryptographic protocol, including the consensus mechanisms to validate transactions and, therefore, to include new registers in the blockchain, and most specifically the immutable register of transactions (blockchain) piece.

The reason is that this piece shows very interesting features, displayed in figure 2, which differentiate it from a traditional database and allow it to be used in innovative ways.

Figure 2

The disruptive features of the blockchain

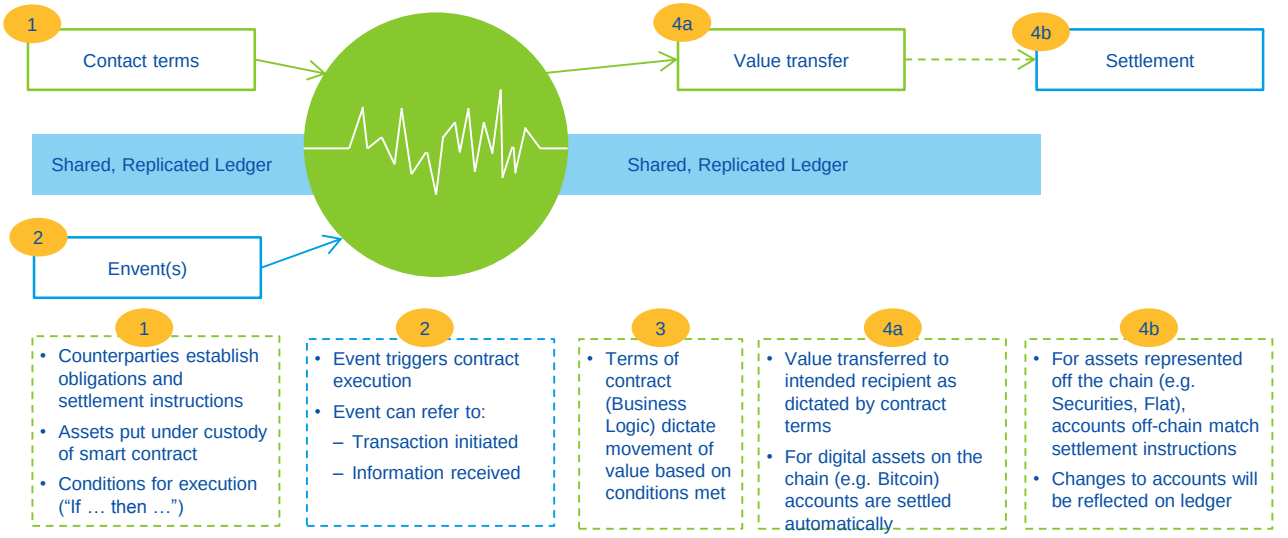


Source: BBVA Research

One of the most promising features is depicted in the lower right box of Figure 2: software programs can be built to leverage the information in the blockchain: these programs are called "smart contracts" and are basically computer code uploaded to a ledger, rather than basic passive data entries. Smart contracts are programmed to generate instructions for downstream processes (such as payment instructions or moving collateral) if reference conditions are met. Like passive data, they become immutable once accepted onto the ledger. The basic functioning of a smart contract can be seen in Figure 3.

Figure 3

Applying business logic with smart contracts



Source: BBVA Research, based on Jo Lang / R3 CEV

Most of these concepts (cryptocurrencies, immutable distributed ledgers, smart contracts) represent a radical shift with respect to the usual way of thinking about the foundations not only of financial systems but also of law, commerce, economy, society and trust itself.

2. Regulatory landscape

As in any new technology, opportunities that distributed ledgers bring are accompanied by important challenges that are going to influence on their massive adoption. Some of the most relevant ones have to do with the way they are going to be regulated, bearing in mind that a technology, by definition, is not object of regulation, but the different uses of the technology. In the case of blockchain, the exploratory phase in which we currently are makes even more difficult to undertake its regulation.

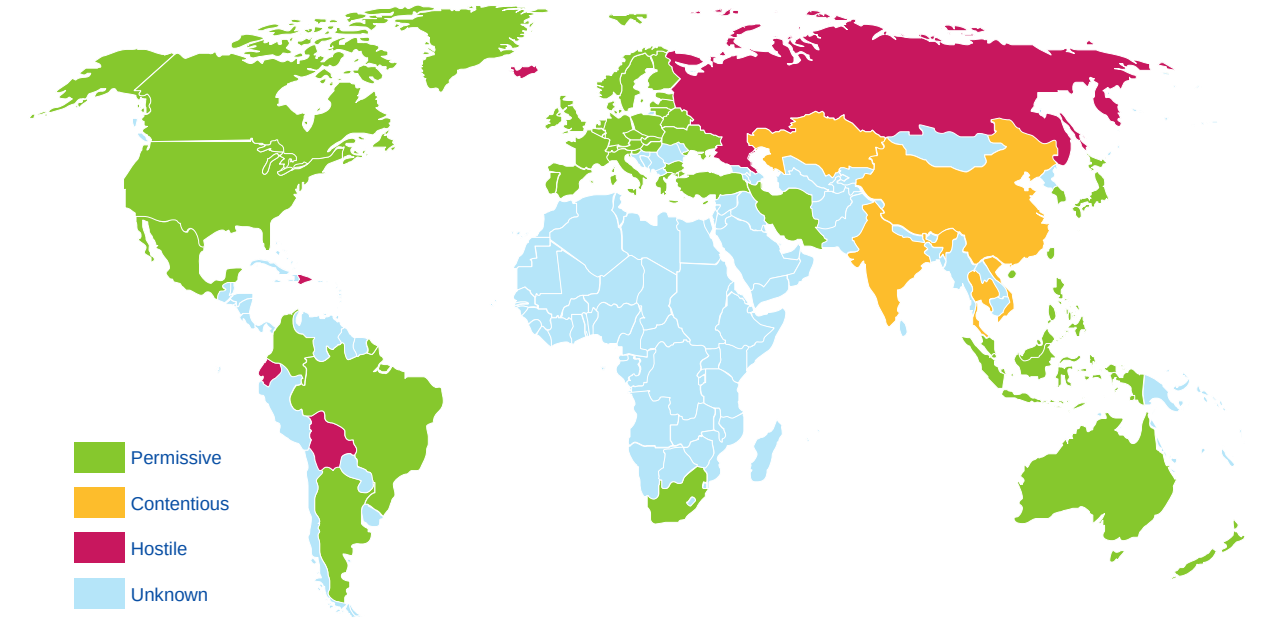
The current regulatory landscape when talking about DLTs is simultaneously immature and complex, and it depends on what component of the DLTs we are talking about: cryptocurrencies, blockchains, shared ledgers, smart contracts, etc. The regulatory treatment of each of these components is different, although lack of specific regulation is a common factor.

Being cryptocurrencies, and specifically bitcoin, the only active use case in the real world involving a significant number of user, the first regulatory initiatives are focusing in this field: legality of their use, consideration from the point of view of taxation, and avoidance of illicit activities related to these currencies are the first topics that have been addressed by policymakers and regulators.

Regarding the legality of their use, there are few countries clearly against them. Figure 4 shows a map with a representation of the attitude of countries with respect to the use of bitcoin: we can see that most countries are permissive.

Figure 4

Attitude of countries with respect to bitcoin



Source: Bitlegal.io

A different matter is how countries are considering cryptocurrencies from the point of view of taxation: some countries consider them as digital money, while others treat cryptocurrencies as digital products or commodities. In this sense, a significant step was given in October 2015 when the European Court of Justice (ECJ) ruled that bitcoin exchange transactions should be exempt from value-added tax (VAT). The ECJ ruling stated that bitcoin transactions "are exempt from VAT under the provision concerning transactions relating to currency, bank notes and coins used as legal tender."[1] This ruling in fact means that bitcoin is treated as money, changing previous Member States' rules (i.e. in Germany it was considered a commodity).

As an example on the other direction, regulators in the US have different criteria about bitcoin: some consider it as money (FinCEN, SEC), while others consider it a commodity (CFTC), or even a property (IRS, Internal Revenue Service)[2]. This leads to discretionality of judges when a bitcoin-related lawsuit goes to court.

Anyway, from a global perspective, regulatory initiatives around the broad field of distributed ledger technologies are in their first stages all around the world. Although, especially in the last year, most regulators have set up working groups and taskforces to analyse the topic, there are still really few tangible steps towards an enforceable regulation.

A non-exhaustive summary of initiatives and pronouncements by different authorities around the world is compiled in the table below. Note that a "negative" or "neutral" position means that the authority focuses more on the risks than in the benefits, but it does not represents an actual opposition to the use of virtual currencies or DLTs.

1: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150128en.pdf
2: http://bravenewcoin.com/news/bitcoin-is-officially-a-commodity-first-cftc-ruling-against-a-bitcoin-options-trading-platform/

Details of the different geographies and authorities can be found in the Annex I at the end of the document.

Table 1

Position of relevant authorities on virtual currencies and distributed ledgers

Authority	Geography	Position	Format	Topic	Summary
Policymakers					
European Parliament	EU	Neutral to Positive	Report / Taskforce	Virtual Currencies / Distributed Ledgers	Hands-off approach to regulating blockchain technology. Creation of a task force to analyse it
European Commission	EU	Neutral	Directive / Taskforce	Virtual Currencies	Inclusion of virtual currencies players in the AML Directive. DLT workstream inside the Financial Technology Task Force
US Senate	USA	Neutral	Letter to regulators	Virtual Currencies / Distributed Ledgers	Request to regulators for guidance on these technologies
US House of Representatives	USA	Neutral	Non-binding resolution	Virtual Currencies / Distributed Ledgers	Resolution calling for a national technology innovation policy including digital currencies and blockchain technology
US Congress	USA	Positive	Study group set-up	Virtual Currencies / Distributed Ledgers	Creation of a caucus (study group) dedicated to bitcoin and blockchain
State Governments	Several US states	Positive	Regulation	Virtual Currencies / Distributed Ledgers	New York, North Carolina, Vermont and Delaware have promulgated specific regulations
Financial Authorities					
EBA	EU	Negative to neutral	Reports	Virtual Currencies	Recommendation to banks not to deal at all with virtual currencies, and amendments to the EC decision to include virtual currencies players in the AMLD
ESMA	EU	Positive	Public Consultations	Virtual Currencies / Distributed Ledgers	Consultations on investment using virtual currency or DLT and on DLT applied to securities markets
FinCEN	USA	Neutral to Negative	Report	Virtual Currencies	Guidance to avoid illicit activities through the use of virtual currencies
CFPB	USA	Neutral to Negative	Report	Virtual Currencies	Statement about big issues have yet to be solved regarding virtual currencies
OCC	USA	Positive	Report	Distributed Ledgers	Statement about how DLT has the potential to transform how transactions are processed and settled
CFTC	USA	Positive	Declaration	Distributed Ledgers	Statement about how blockchain may give regulators transparency
SEC	USA	Neutral	Declaration	Distributed Ledgers	Statement about the commitment of the agency in actively exploring blockchain regulation
Federal Reserve	USA	Positive	Declaration / Report	Virtual Currencies / Distributed Ledgers	Statement about how blockchain may represent the most significant development in many years in payments, clearing, and settlement. In the context of payments, DLT has the potential to provide new ways to transfer and record the ownership of digital assets; immutably and securely store information; provide for identity management; and other evolving operations through peer-to-peer networking, access to a distributed but common ledger among participants, and cryptography
FCA	UK	Positive	Declaration / Sandbox Initiative	Distributed Ledgers	Statement about considering approving blockchain-based firms into their Sandbox Initiative (finally, 9 out of 16 approved firms use DLT)

Continued on next page

Table 1 (cont.)

Position of relevant authorities on virtual currencies and distributed ledgers					
Authority	**Geography**	**Position**	**Format**	**Topic**	**Summary**
Central Banks					
ECB	EU	Positive on DLT, Negative on VC	Reports / Declaration	Virtual Currencies / Distributed Ledgers	The ECB has analyzed virtual currencies and identified potential risks. In fact, it has warned the EC not to encourage the use of virtual currencies in order to keep controlled money issuance. On the other side, it sees potential benefits in the use of distributed ledgers in post-trading activities. And it has started a joint project with Bank of Japan to analyze potential use of DLTs.
National Central Banks	Several countries	Positive	Declaration / BoE report	Virtual Currencies / Distributed Ledgers	A number of central banks have stated serious interest in the issuance of their own currencies. The Bank of England have published a paper on this topic
International Finance institutions					
FATF	Global	Neutral to Negative	Report	Virtual Currencies	Recommendations for avoiding illicit activities related to virtual currencies
FSB	Global	Neutral to Positive	Declaration	Distributed Ledgers	Statement including distributed ledger technology among their priorities for 2016
OICV-IOSCO	Global	Neutral	Declaration	Distributed Ledgers	Committed to analyse the impact of blockchain in the framework of their Securities Markets Risk Outlook
BIS	Global	Neutral to Negative	Report	Virtual Currencies	Statement about the effect of digital currencies in reducing role of central banks
IMF	Global	Positive	Report	Virtual Currencies / Distributed Ledgers	Publication of specific reports on virtual currencies and distributed ledgers (considering them as “The Internet of Trust”)
World Bank	Global	Positive	Article	Distributed Ledgers	Article analysing how blockchain technology redefines trust in a global digital economy
International Consultative Bodies					
WEF	Global	Positive	Report	Distributed Ledgers	Statement about how blockchain will become “beating heart” of the global financial system

Source: BBVA Research

3. Blockchain as a tool for regulators and supervisors

Distributed ledgers have intrinsic advantages: instant settlement, easier and more trustworthy management of collaterals, monitoring of OTC operations invisible today to the market, lack of need of clearing houses, more globalization, more effective supervision, and so on.

But there are challenges to solve related to the kind of legal entities these permissioned distributed ledgers will be, and how future industry consortia will interact with regulators. A nascent idea is that the regulator acts as another node of the network, so it has real-time access to the ledger, either in read-only mode or with more attributions.

Now, this idea brings along some additional questions, as there can be multiple consortia, and they usually will have a global approach, because by nature distributed ledgers are not tied to specific geographic locations. But regulatory requirements in most cases have a local component. So, what regulators are going to be included in what consortia is an issue to solve. And most importantly, how will those international or local regulators coordinate themselves?

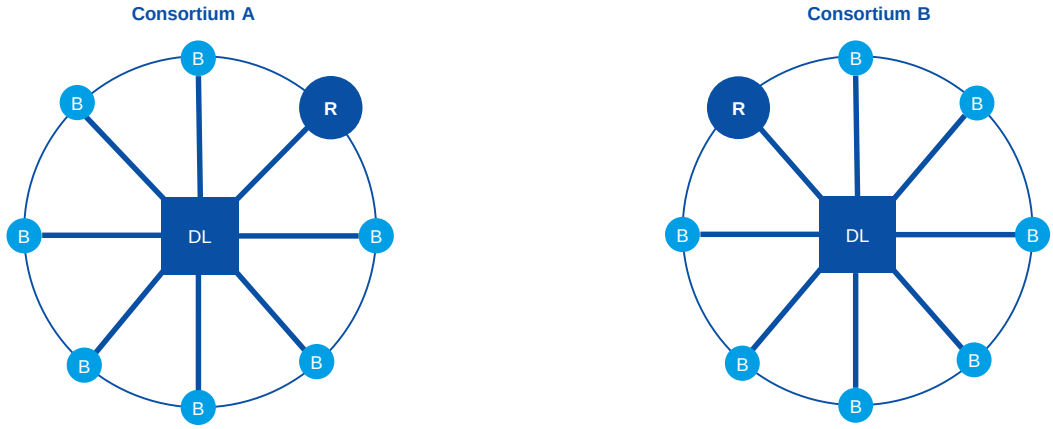
Option 1: the supra-regulator

One option for the role of regulators in consortia would be the creation of a supra-regulator. This omniscient regulator will be global and will have a reserved node in each and every consortium in the financial industry, with unlimited access to all the relevant information needed to assess systemic risk.

It is highly improbable that this kind of simple approach becomes reality (except in the case of currently non existent national consortia, where central banks would have the whole authority), because regulations currently have a strong geographical component, and local and regional specificities have to been taken into account.

Figure 5

Role of regulators in consortia: the supra-regulator



Source: BBVA Research

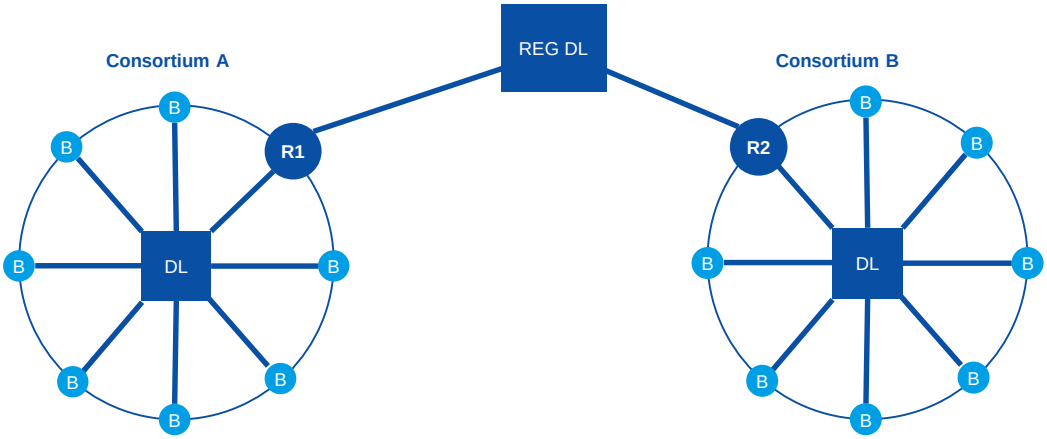
Option 2: the regulator's DL

The second option for the role of regulators in consortia would be the creation of regional consortia. Thus, each consortium would have nodes for the regulators to which the entities of that particular consortium have to answer. Then, all those regional regulators could share information in real time through their own distributed shared ledger, and global regulators, if any, could have access to this regulators' DL.

This approach is feasible but difficult as it is not the direction in which consortia, that for now are global, are moving. Regional consortia are possible that could be interconnected by protocols linking ledgers, as Interledger, so in spite of being regional, the whole system would be global.

Figure 6

Role of regulators in consortia: the regulators' DL



Source: BBVA Research

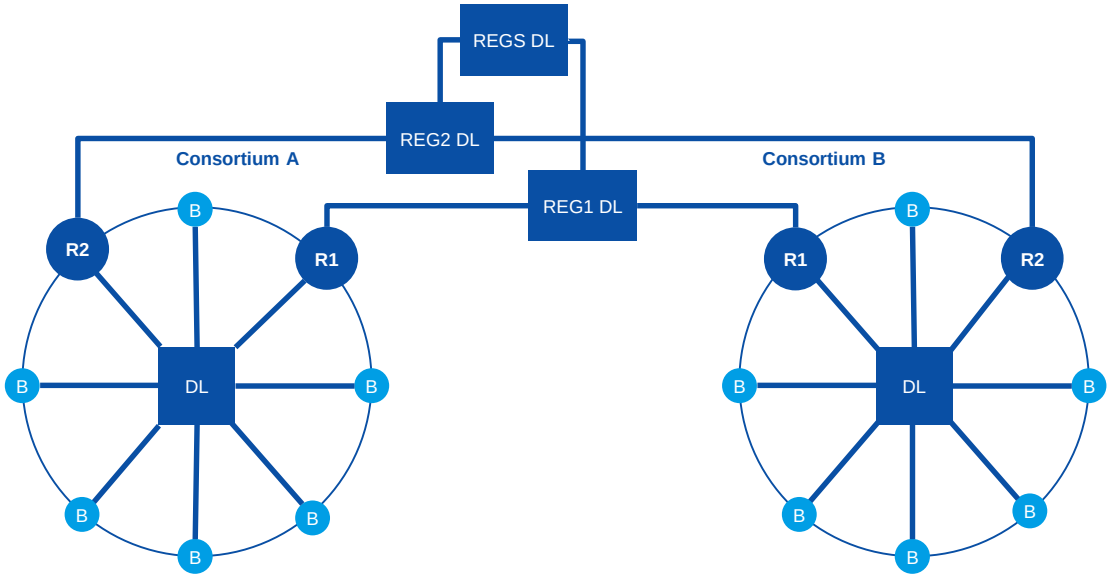
Option 3: the levelled regulator's DL

The third option for the role of regulators in consortia is the "levelled regulators' DL". In this case, regulators from different geographies have presence in each of the global consortia, accessing only to the information needed to perform their supervision activities related to the entities that fall under their jurisdiction. Then, information extracted by one regulator from every consortia it is in, is shared in a private ledger. Thus, regulator 1 would have a ledger with all the information it has extracted from consortia A and B. Same for regulator 2 and so on. Finally, all the regulators form their own network where they share a regulators' ledger to combine all the information needed for the monitoring of the global systemic risk.

This approach seems to be the one we are moving to. Consortia are reserving specific nodes for different regulators in their networks, and R3 even is talking about a future "regulators network" that hasn't been defined yet but could possibly work in this way.

Figure 7

Role of regulators in consortia: the levelled regulators' DL



Source: BBVA Research

4. Main regulatory challenges ahead of blockchain

Blockchain is a technology, and by principle technologies themselves cannot be regulated, but activities performed using those technologies. In the case of blockchain, the immaturity of the initiatives and the piloting phase of identified use cases has made that **regulation of blockchain activities in the financial services industry is still non-existent**, Given that **regulation of activities over the blockchain depends on the field of the activity**, there's few to say about general regulatory claims from the incumbents in the industry, except requesting the regulators a **"level playing field"** to compete with the new blockchain startups, and the option to create **"regulatory sandboxes"** to pilot potential activities of the technology without colliding with current regulations.

However, there are **some current regulations that will apply to blockchain-based services**. For instance, any smart contract defined on the blockchain will have to comply at least with the regulation on contracts applicable on the correspondent jurisdiction, as exposed in the commercial and trade law.

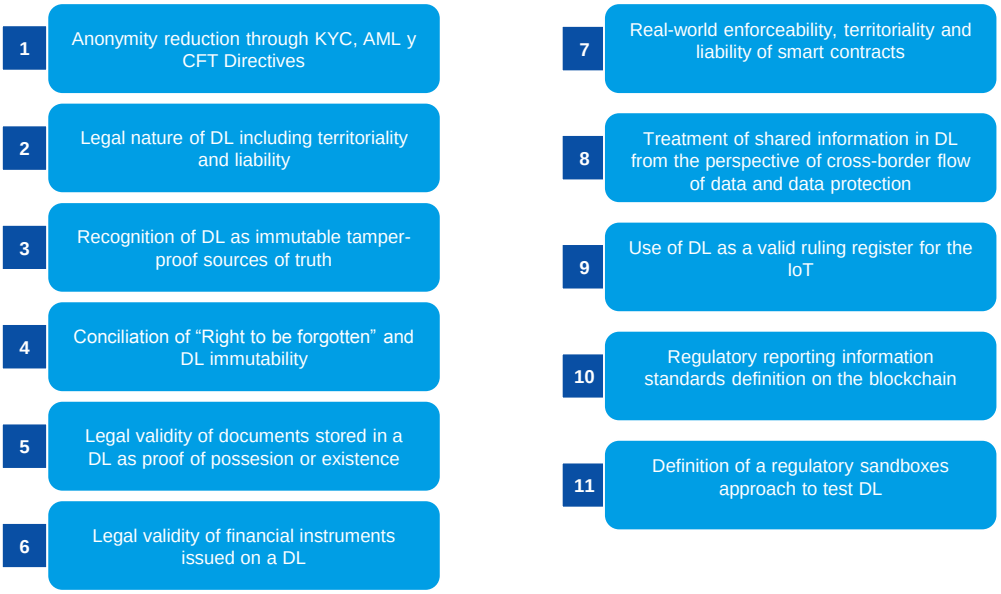
Then, **depending on what kinds of financial services are being offered on the blockchain (payments, lending, investment, etc.), regulation on these services will have to be applied**. For instance, KYC and AML regulation, capital markets regulation, lending regulation, and so on.

Anyway, close collaboration with regulators and supervisors from the beginning is necessary to adapt and develop consistent regulations regarding blockchain technologies.

And, in the end, when watching at the big picture in blockchain, there are a number of transversal challenges that, regardless of the use case, are going to be present and that will have to be addressed at some point in the future. We have identified eleven of these challenges.

Figure 8

Distributed Ledgers (DL) main regulatory challenges



Source: BBVA Research

1. **Inclusion of payments and international transfers service providers using blockchain technologies in KYC, AML / CFT Directives** in order to ensure a level playing field and control potential illicit uses of cryptocurrencies. Exchange platforms and custodian wallet providers are already proposed to be included in the 4th AMLD by the European Commission on July 2016.

   The EBA has published its opinion about this proposed amendments to 4AMLD clearly supporting the adoption of a dedicated regulatory framework relating to virtual currencies, but with nuances that have already been mentioned above.

   In a legal opinion published afterwards, the ECB said EU institutions should not promote the use of digital currencies and should make clear they lack the legal status of currency or money. The ECB opines that the reliance of economic actors on virtual currency units, if substantially increased in the future, could in principle affect the central banks' control over the supply of money ... although under current practice this risk is limited.

   The ECB also argues the Commission's proposal does not go far enough as it does not cover the use of virtual money to buy goods and services. The ECB says that such transactions would not be covered by any of the control measures provided for in the proposal and could provide a means of financing illegal activities.

2. **Legal framework regarding the legal nature of blockchains and distributed ledgers** in general, including territoriality (jurisdiction issues and applicable law) and liability (responsibility when something goes wrong).

   By definition, distributed ledgers are not subject to a specific location. In terms of jurisdiction and applicable law, territoriality is an issue, because every node of the network can be subject to a different law, and there is not a "central party" responsible for the ledger, whose nationality could serve as an "anchor" for regulation. Following the same reasoning, liability is a concern, because there could not be an ultimate responsible for the functioning of the ledger, and the information that is inside it. This is obviously true in the case of public distributed ledgers, but in the case of "federated" ledgers it would depend on if the ledger itself is going to have any kind of underlying legal entity or not. An ad-hoc company or legal entity created to manage the ledger would ease these liability and territoriality issues.

3. **Legal framework for the recognition of blockchains as immutable, tamper-proof sources of truth** regarding the information stored on it. Related to this, legal framework for the use of blockchains as single sources of trusted identity as well. Harmonized regulation about data protection and definition of identity in the case of legal persons will be needed as a previous step.

   Although there is a wide consensus among cryptography and information technology communities about the practical immutability of the blocks in a well-defined blockchain, being due to the computational unfeasibility of changing blocks in "proof-of-work" schemes or to another kind of controls linked to different consensus mechanisms, there is still a lack of legal recognition of this characteristic of the blockchain and therefore it cannot be used as an argument in front of any court yet. As of today there is not any resolution made by a court in the world that recognizes the blockchain as immutable, tamper-proof sources of truth.

   A related topic comes to first line when the information stored in the blockchain is identity information. The use of blockchains as potential "single sources of trusted identity" is the ultimate goal of many players in the ecosystem and could represent a definitive step towards a "universal identity" on the Internet. But a previous requirement is the recognition of blockchains as immutable sources of truth. And, of course, another previous issue to address is the definition of identity in the case of legal persons, something that is already on going through the definition of the LEI (Legal Entity Identifier). Related harmonization in regulation about data protection is being included as another challenge.

4. **Regulation on how the "right to be forgotten" shall be interpreted**, because the tamper-proof feature of the blockchain collides with this right recognised by European regulation on personal data protection.

   The inherent immutability of the blockchain can represent an issue when it collides with rights recognized previously by policymakers, governments and/or regulators. A clear example is the "right to be forgotten" recognized by European regulation to every citizen, meaning that any European citizen has the right to have their personal information deleted from some second party's electronic or paper records or databases.

Although this right doesn't exist in the same terms in other jurisdictions like the US, it is something to have in mind when trying to use blockchain technologies to store personal information, because information in the blockchain cannot be deleted. Accenture has announced patents on editable blockchains, but an editable blockchain is just like a traditional database so we are not including this kind of blockchains in this analysis. In addition, discussion about editable vs. non-editable blockchains exceeds the limits of this document.

The only potential solution to reconcile this kind of rights with the nature of the blockchain could be to substitute the right to "deletion" by the right to "impossibility of use" of personal information by third parties. This could be achieved by a combination of automatic encryption of information when certain conditions are met (a smart contract will be involved) or alternative solutions to prevent access to that information when the citizen decides to claim his right.

5. **Legal framework about the legal validity of documents stored in the blockchain as a proof of possession or existence.**

Similarly to the recognition of the blockchain as an immutable single source of truth, there is a second level of recognition needed prior to use blockchains in certain kinds of businesses. It is not only the recognition that the information cannot be changed, but the recognition that the inclusion in the blockchain of a document representing ownership or existence of an asset really proves the real ownership or existence of that asset.

However, if the process of verifying that ownership/existence prior to the inclusion of the document in the blockchain is robust enough, and we trust on validity of cryptographic functions used in blockchain technology, then the recognition of the blockchain as immutable source of trust implies that the documents in the blockchain really could be used as a proof of existence or ownership. A different thing is at what extent any court in the world recognizes this. Again, there is not jurisprudence in this regard.

The definition of this legal framework has direct implications, of course, on land registries and other registries currently used to ensure and monitor ownership on the public administration side.

6. **Legal framework about the legal validity of financial instruments issued on the blockchain**

When trying to use the blockchain as a platform to define "native" financial instruments, like bonds or derivatives, it is needed a recognition of the legal validity of these financial instruments by the corresponding regulators and supervisors. As we have seen before, the Bank of France has already taken a step forward in this regard recognizing certain mini-bonds issued directly on the blockchain.

A harmonized approach by international regulators is needed, however, if we want this practice to be globally adopted. And the analysis of the implications of the existence of these instruments on the financial system are still pending.

The ultimate case of financial instrument issued on the blockchain would be, of course, money. Native money issued on a blockchain could have a huge impact on monetary policies and macroeconomics, and deserves a more in-depth analysis that is beyond the limits of this document.

7. **Legal framework for smart contracts** in general, and in international commerce in particular, including real-world enforceability, territoriality and liability.

   Smart contracts are one of the most interesting concepts surrounding blockchains and, at the same time, one of the most challenging from the regulatory point of view. Issues mentioned in the point 2 above regarding territoriality and liability are applicable to smart contracts as well, but with additional considerations.

   First, regarding jurisdictional issues. It is not only that the ledger itself has not specific location, but also in addition parties signing an agreement can be subject of different laws in their respective jurisdictions.

   Second, regarding liabilities. Smart contracts have multiple parties involved: not only the contracting parties, but also the contract creator (usually some kind of coder) and the contract custodian (although this last party could be avoided in an ideal case). Then, apart from the obvious possibility of one of the contracting parties not complying with the contract, there is a chance of the smart contract itself working badly, due to mistakes in coding or defects in design (see the recent DAO case where someone found a way to “steal” money while being comply with the contracts).

   Thus, when a smart contract performs in a wrong way, which party is responsible for that?

8. **Legal framework for the treatment of shared information in blockchains from the perspective of cross-border flow of data, and data protection** in general.

   The distributed and shared nature of blockchains has direct implications on the management of data stored in. On one hand, although in the initial design of the bitcoin blockchain information in the ledger is accessible to all the nodes of the network, when designing specific use cases, and specially when using “consortiated” ledgers, there has to be a careful management of the “slices” of information accessible to each participant in the network. Initiatives like Corda from the R3 consortium are designed so only the parties involved in a transaction can see the details of the transaction. Approaches as “zero-knowledge proof” (a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, without conveying any information apart from the fact that the statement is indeed true) can be put in place to solve privacy issues.

   Also, as mentioned in other challenges, there is the territoriality question, that affects data as well. Information in the ledger is decentralized and this means that there is an inherent cross-border data flow that can be against existing regulations.

9. **Legal framework regarding the use of the blockchain as a valid ruling register for the IoT**

   An intriguing use of the blockchain has been said its application to the Internet of Things (IoT). Since in the IoT realm everything has an identity, it would be really useful to have a common shared register to store things "identity" and information, and to allow transactions between them, including M2M payments.

   This idea of one or many interrelated "director ledgers" for the IoT is barely nascent and if it comes to practice it will be in a long term, but anyway it will require the existence of a legal framework in which this director ledgers be recognized as valid ruling registers for the IoT. All the challenges previously mentioned about territoriality, liability and enforceability of smart contracts are of course applicable to these blockchains associated to the functioning of the IoT.

10. **Regulatory reporting information standards definition on the blockchain**

    Recent research about RegTech, or technologies applied to the addressing of regulatory requirements, show that blockchain technologies can be useful tools for that. Having all the transaction information in a shared register in almost real time could allow regulators and supervisors to monitor financial activity without having to wait to receive the required reports from the financial institutions, and to have in the future a real time global vision of systemic risk.

    For this to happen, a set of standards about what kind of relevant information about the transactions have to be stored in the ledger(s), and in which format the information have to be in that register so regulators can easily extract the needed data. Also, there has to be a clear definition of the clusters of information that each regulator or supervisor must have access to, especially in consortia where there are special network nodes for regulators.

11. **Definition of a regulatory sandboxes[3] approach** 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 otherwise breach them. If there is not a clear breach involved, issuance of 'no enforcement action letters' and individual guidance to firms on the interpretation of rules.
    - Alignment of the sandbox rules to local and EU legislation.

3: A regulatory sandbox is a controlled environment in which firms can test innovative solutions with real customers without immediately incurring the entire normal regulatory burden.
Regulatory sandboxes allow firms trying to innovate (both startups and incumbents) to test new technologies, solutions and business models in real life environments sooner and at a lower cost. For authorities, sandboxes allow a better understanding of innovations before providing regulatory guidance or proposing regulatory changes.
Regulatory sandboxes should be ruled by clear ex-ante principles to ensure fairness and avoid arbitrariness, yet flexibility is also needed to quickly address the specificities inherent to any innovation. In addition, the sandbox must ensure a level playing field between new players and established firms that are already authorized: to that end, a minimum set of requirements should be established for all participants. Also, different regulatory and supervisory bodies (prudential, consumer protection, data protection, AML/CFT, etc.) should be involved to ensure the sandbox is really effective. Of course, sensitive data about the innovations that apply and/or participate in the sandbox should remain confidential between the firm and the authorities. Finally, fundamental customers rights and the integrity of the financial system should never be eroded during the sandboxing activities.

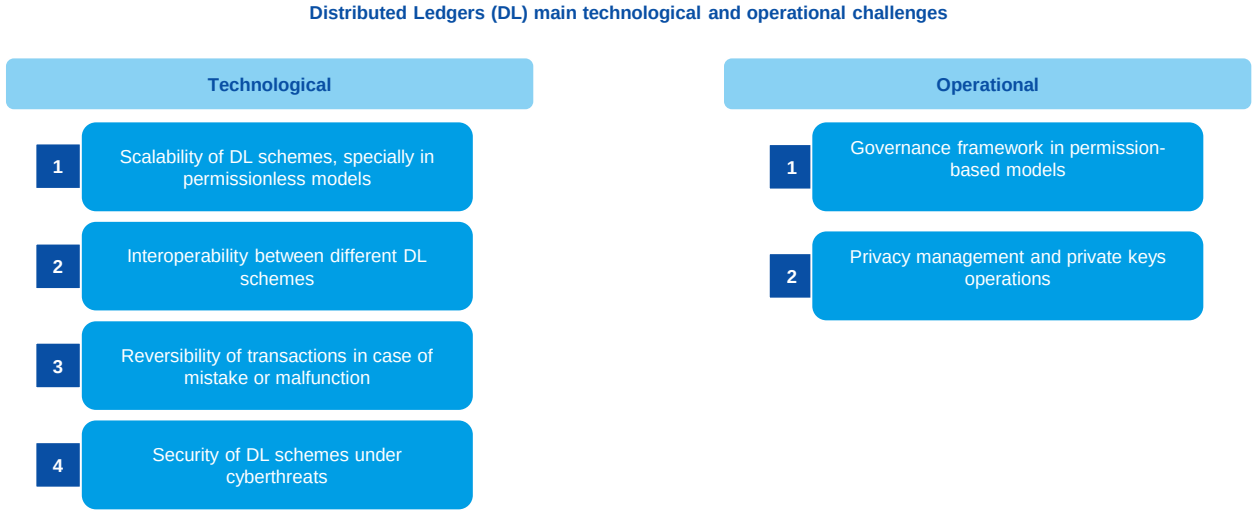
- Consumer safeguards, include limiting testing activities to customers who have given informed consent to participate, providing customers of sandboxing firms the same rights as customers of other authorised firms, requiring firms in the sandbox to have the resources to compensate any losses to customers or agreeing on a case-by-case basis the disclosure, protection and compensation appropriate to each testing activity.

5. Other technological and operational challenges of blockchain

In addition to the direct regulatory challenges identified above, there are a number of technological and operational challenges that in the future could arise new regulatory questions. These other challenges have to be bore in mind in order to anticipate the potential future needs with respect to modifications to current regulations, as in the case of cybersecurity, privacy or net neutrality (associated with scalability efficiency).

Figure 9

Role of regulators in consortia: the regulators' DL



Source: BBVA Research

Technological challenges

- **Scalability.** Technology is not scalable at this point, especially when talking about permissionless schemes based on proof-of-work consensus (like bitcoin), due to predetermined size of block and energy consumption issues. In the example of Bitcoin and despite extensive amounts of computing power, the network is restricted to 7 transactions per second, as all nodes need to process all transactions. Under these circumstances it is difficult to build practical use cases for financial services. Nevertheless, entry of big technological/Internet firms (IBM, Microsoft, Amazon, etc.) into the field will help to solve this issue. And in the case of permissioned schemes, scalability probably will not be an issue at all.

  As an example, the Raiden Network is an extension to Ethereum under development that scales linearly with the number of participants allowing 1,000,000+ transfers per second.

- **Interoperability.** As DLTs will probably be used firstly in niche applications, they would need to interoperate with existing infrastructures. Also, there will be different ledgers for different asset types (or even industries) that will need to interact with one another. There are technical challenges that can only be relief by the adoption of common standards by all the players in the field.

  Both the ISO and the W3C are working on standards for interoperability of ledgers. And there are private initiatives, like Interledger, focused in this issue

- **Reversibility.** In its current design, the DLTs creates immutable shared ledgers, in which transactions cannot be modified, cancelled or revoked. This poses the challenge of how to handle potential mistakes from a technological and also governance perspective, e.g., who would be entitled to flag errors, which correction mechanism would then apply and according to which timeframe. And because the DLTs could potentially increase the speed of clearing and settlement, there is heightened need to quickly correct mistakes.

  Also, when a security breach happens due to final user's credentials are leaked, the consequences are much more severe and difficult to resolve than in a centralized scheme, because the decentralised chain design means that it is not possible to simply revert previous actions.

- **Security:** Blockchain technologies present some traditional security challenges, and new ones coming from their own nature. Regarding traditional challenges, distributed ledgers remove a "trusted central party", displacing the potential breach points to the end users. This means that although a transaction is verifiable by all other entities on a ledger, nothing assures that the owner of the wallet has not been victim of a hack. Therefore, the principles and concerns of securing any user's account on a traditional system, usually of usernames and passwords, are still largely the same as ensuring the security of the user's private key.

  On the other side, most known Blockchains rely on the cryptographically generated public and private keys of their users to operate. New technologies such as quantum computing threaten the premise of asymmetric cryptography by allowing hugely faster calculations. Though this exponential computing capability poses mainly a long-term threat, there are a number of post-quantum algorithms being researched that, so far, are theoretically resistant to the capabilities of a quantum computer.

  Also, as with all systems, there remains the latent, so far undiscovered vulnerabilities in the Blockchain system. Whilst many skilled eyes have reviewed the protocols, methods, and codebases of the most popular implementations of distributed ledgers, it still remains possible that zero-day vulnerabilities exist.

  In decentralized, permissionless networks, where consensus is formed through majority participation, hijacking of a large enough portion of the miners could raise the possibility of the attacker affecting the validation process. In the case of Bitcoin, this is referred to as a "51% attack" where the majority (defined as the proportion of all hashing power in the network) is compromised or controlled by the same entity or a coalition of dishonest counterparties. Similarly, in a regulated, permissioned network, where consensus might be implemented under the regulator's direction, any exploitation of the regulator's capabilities would be even more and immediately severe. All of the problems that before required hijacking of the majority consensus, a task that was a potentially significant undertaking, are now replaced by the hijacking of a single operator.

There are also potential vulnerabilities related to the transaction protocol and the possibility of fraudulent transactions (double-spending in certain cases, transactions initiated with hacked keys, or, in permissioned networks, transactions non-compliant with the rules of the ledger). Distributed Denial of Service attacks, where rogue wallets will push large numbers of spam transactions to the network, remain a concern too.

The distributed nature of Blockchain architecture also introduces the prospect that it would be difficult to shut down a malicious program. With the capabilities of newer protocols offering data storage and computation, it would be possible to store a worm's data within the Blockchain.

Additionally, there are the issues created by smart contracts. These are found in the execution of code, the function and security of that code being dependent upon the author's capabilities. A review by Peter Vessenes found that large swathes of template contracts available on the web for the Ethereum scripting system contained significant, if not fatal vulnerabilities to their operation. One significant demonstration of this is the June 17th 2016 attack on the DAO, an investment vehicle created on the Ethereum network and operated as a smart contract. Over $59m in Ether were stolen by an unknown source from the wallet controlled by the program on behalf of all investors.

Another key problem is a lack of tools to combat illegal activity. Though it might be possible to identify who owns an address used for money laundering despite attempts at obfuscating the transaction, it is not possible to block these types of transactions in advance.

Operational challenges

- **Governance framework.** The DLT that is likely to be applied to financial services would be 'permission-based' in contrast to a 'permissionless' system (like Bitcoin) due to efficiency, security and privacy reasons. A permission-based framework requires rules to approve/reject authorised participants, including perhaps minimum capital requirements, conduct of business rules and risk management processes. In addition, rules to govern the interactions between participants, both 'permissioned' and 'non-permissioned' will be necessary. Examples include the liabilities of the respective participants, including in case of fraud or error, correction mechanisms and penalties in case of infringement to the rules, the intellectual property attached to the technology or the territoriality of the law likely to apply to the network. An agreement between the participants on their remuneration model would also be needed. Furthermore, the governance framework should provide clarity on the entity or group of entities that would be held liable for the activities of the network vis-à-vis third parties, in particular local regulators and customers.
- **Privacy management.** By design, the information recorded on DLs is made public to the participants of the network, or at least to 'permissioned' participants. This information typically comprises the history of the transactions and the balance of cash and assets held on accounts. In addition, it seems that the DLTs could be used to store and share private information on clients, e.g., for KYC procedure purposes. The question is how to combine the public nature of the ledger with the need to preserve the anonymity and privacy of some of the information recorded. The use of encryption identifiers (i.e. private keys) instead of names could provide some level of privacy, but the operation of those private keys would need to be carefully designed and controlled.

Conclusion

Distributed ledger technologies, including blockchains, are in a stage-changing moment. From the initial embryonic stage in which the tech-savvy community was the main (if not unique) player in the field, we are now reaching a second stage, in which businesses are starting to analyse the specific use cases for the technology.

At this point, regulatory issues that were, to a certain extent, ignored due to the impossibility to regulate technologies, are moving into the spotlight because they must be studied and solved to allow the massive adoption of distributed ledgers. Of course, technological, operational and business challenges are still there, and they must be addressed as well, but a proper regulation will be essential for the future of DLTs.

Regulatory challenges are multiple and will have a deep impact, not only on current regulations or even in new regulations inside the current regulators' mindset, but they could mean a change in that mindset itself. Distributed ledgers, blockchains, smart contracts and other related concepts are a different kind of legal objects that in most aspects can collide with the current legal framework, since they don't easily fit in the traditional concepts of jurisdiction, liability, or enforceability. As an example, extreme blockchain-based automation could lead to autonomous entities whose legal definition will not be easy using traditional legal parameters.

In summary, dealing with DLTs will probably require a redefinition of some fundamental foundations of law, and a reconversion of lawyers, regulators and policymakers, that will need to acquire new technology-related skills in order to be able to interpret a new world of decentralized autonomous businesses governed by automated relationships.

Annexes

Annex I: Regulatory and public policy initiatives by geographies

Europe

The European Parliament is taking a hands-off approach to regulating blockchain technology. European Commission staffers are working hard to understand the distributed ledger technology behind virtual currencies. A new task force has been created[4], which would be overseen by the European Commission, which should build expertise in the underlying technology of virtual currencies.

The European Commission proposed in July 2016 to bring virtual currency exchange platforms and custodian wallet providers within the scope of the 4th Anti-Money Laundering Directive. In October 2016, the **Council of the European Union** published a Presidency compromise text on the proposal[5].

In November 2016 the Commission decided to set up an internal Task Force on Financial Technology (FTTF).[6] One of the defined workstreams of this FTTF is dedicated to Distributed Ledger Technologies.

European regulators and supervisors like the ECB, the EBA and the ESMA are showing a growing interest in blockchain technologies. All of them have published different papers and consultations on virtual currencies and DLTs.

- **ECB (European Central Bank):** In February 2015, the ECB published a report titled "Virtual currency schemes – a further analysis"[7] focused on the currencies themselves. More recently, its interest has shifted to distributed ledgers, and in April 2016 a new report on DLs applied to post-trading activities entitled "Distributed ledger technologies in securities post-trading"[8] has been published.

  On December 6th 2016, Yves Mersch, Member of the Executive Board of the ECB, gave an speech called "Distributed Ledger Technology: role and relevance of the ECB"[9] in which he expressed the recognition of DLT as something that could radically alter the financial ecosystem as we know it and the will of the ECB to keep assessing its potential applications, even launching a joint project with the Bank of Japan to analyze the technology. However, he stated as well that DLT is in its relative infancy and it is too early to say with any certainty whether and how it could change the ecosystem.

- **EBA (European Banking Authority):** in July 2014, the EBA published its "Opinion on 'virtual currencies'"[10] in which it recommended banks not to deal at all with such currencies. Recently, in August 2016, as a reaction to the decision of the EC to include virtual currencies in the AMLD, the EBA published their

4: http://www.coindesk.com/eu-parliament-digital-currency-task-force/
5: http://data.consilium.europa.eu/doc/document/ST-13872-2016-INIT/en/pdf
6 https://ec.europa.eu/digital-single-market/en/blog/european-commission-sets-internal-task-force-financial-technology
7: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf
8: https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf
9 https://www.ecb.europa.eu/press/key/date/2016/html/sp161206.en.html
10: https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

"Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD)[11]" in which they mention the following points:

- The EBA asks for a longer deadline for transposition (June 2017, instead of January 2017) so VCEPs (Virtual Currencies Exchange Platforms) and CWPs (Custodian Wallet Providers) have enough time to facilitate the adoption of a consistent approach, and Member States can simultaneously create a system for effective supervision and regulation of entities previously outside the Directive's scope, whilst also adopting a new licensing and registration regime.
- The EBA asks for clarification of the VEPs and CWPs regulatory status, particularly where an entity simultaneously provides regulated services and unregulated VEP/CWP activities. The EBA has raised concerns that VEPs and CWPs presenting themselves, intentionally or otherwise, as 'regulated' may be exacerbating a "lack of awareness" as to the AMLD4 amendments' implications. The use of such terminology, which implies a level of regulatory safeguarding that may not exist in reality, exemplifies an indirect consumer risk of VC transactions.
- The EBA suggests that the EU Commission should implement "gateways" that will better facilitate the exchange of information between different Member States' competent authorities responsible for financial regulation. This collegiate approach, it explains, is in-keeping with the international nature of the services that characterise VC businesses.
- Whilst noting that the Commission's proposed amendments require that those holding a management function in, or are beneficial owners of, VEPs or CWPs be "fit and proper" persons, the EBA points out that this requirement is not qualified in any greater detail. Competent authorities should therefore be provided with guidelines as how to carry out 'fit and proper' testing, which will ensure consistency of standards across the EU.
- The Commission's proposed amendments will require VEPs and CWPs to be "licensed or registered". Given the flexibility offered in permitting competent authorities to choose a licensing or a registration regime, there is a risk of confusion and inconsistency of the requirements adopted by each Member State. As well as clarifying the status of VCs as regulated (or unregulated) businesses, and the tests imposed on the "fit and proper" standard, the EBA also calls for clarification on the expected standards of these new regimes, be that registration or licensing.
- Turning to enforcement of the amendments, the EBA supports the resulting extension of sanctions under section 4 of the Directive to be applicable to VCEPs and CWPs. To ensure compliance, the EBA recommends that national authorities be equipped with "effective, proportionate and dissuasive sanctions" to be applied to failures of requirements under the Directive, including, it notes specifically, the reporting of suspicious transactions

11: https://www.eba.europa.eu/documents/10180/1547217/EBA+Opinion+on+the+Commission%E2%80%99s+proposal+to+bring+virtual+currency+entities+into+the+scope+of+4AMLD

- **ESMA (European Securities and Markets Authority):** The ESMA is approaching DLs through public consultations. In July 2015 they closed a "Consultation on investment using virtual currency or distributed ledger technology"; and in September 2016 they closed a consultation based on a "Discussion paper on the distributed ledger technology applied to securities markets"[12]. In November 2016 Patrick Armstrong, Senior Risk Analysis Officer, Innovation and Products Team of ESMA shared some initial conclusions[13] which have arisen from the received answers.

USA

In the USA we have to separate federal regulation from state regulation. Usually federal bodies tend to avoid preemption, because it is unlikely any state agree to federal controls that impact their revenue or their ability to serve its citizens.

Thus, in the field of blockchain, a representative from the **FDIC (Federal Deposit Insurance Corporation)** stated in April 2016 that federal preemption "was unlikely" to be an option, so individual states have to decide how to deal with blockchain. However, federal agencies try to maintain a good relationship with the states and have invited them to tell federal regulators how best to regulate them in order to get a balanced approach to regulation.

In fact, as of today there is not formal regulation at a national level regarding blockchain, even in the cryptocurrency use case, although there are non binding pronouncements from virtually every federal agency stating a position on this topic. **All formal regulatory initiatives have been driven by individual states**.

National level

The first national financial bodies to pronounce about the issue were the FinCEN (Financial Crimes Enforcement Network) in March 2013, and CFPB (Consumer Financial Protection Bureau) in August 2014. Both of them focused on virtual currencies and not on the underlying technology, and highlighted the risks associated to the use of virtual currencies.

Since then, there was a period of absolute silence around the topic. However, in the year 2016, when the blockchain finally exploded among financial institutions, other national agencies like the OCC (Office of the Comptroller of the Currency), the CFTC (Commodity Futures Trading Commission), the SEC (Securities and Exchange Commission) and the Federal Reserve have stated their opinion in a way or another, in most cases by voice of their principal representative. Most opinions are focused on blockchain and are positive in its potential benefits for the financial industry.

The next table compiles the positions stated by different federal agencies regarding bitcoin and blockchain.

12: https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt_0.pdf
13: https://www.esma.europa.eu/file/20549/download?token=8F7yBjha

Table 2

Pronouncements of US National Authorities on Virtual Currencies and Distributed Ledgers

Authority	Date	Type	Topic	Paper / Quote / News Link
FinCEN	March 2013	Report	Virtual Currencies	Guidance on Virtual Currencies and Regulatory Responsibilities
CFPB	August 2014	Report	Virtual Currencies	Risk to consumers posed by virtual currencies "while virtual currencies offer the potential for innovation, a lot of big issues have yet to be resolved – some of which are critical."
OCC	March 2016	Report	Distributed Ledgers	Supporting Responsible Innovation in the Federal Banking System: An OCC Perspective "New distributed ledger technology has the potential to transform how transactions are processed and settled."
CFTC	April 2016	Commissioner declaration	Distributed Ledgers	"[…]if allowed to thrive, blockchain may finally give regulators transparency"
SEC	April 2016	Chair declaration	Distributed Ledgers	"the agency is actively exploring blockchain regulation"
Federal Reserve	June 2016	Chair declaration	Virtual Currencies / Distributed Ledgers	"encourage her counterparts to study emerging technologies, specifically mentioning bitcoin and the blockchain"
US Senate	July 2016	Senators' letter to regulators	Virtual Currencies / Distributed Ledgers	"requesting information about the regulation and oversight of virtual currencies and blockchain technologies"
US House of Representatives	September 2016	Non-binding resolution	Virtual Currencies / Distributed Ledgers	"calling for a national technology innovation policy that includes supportive language for digital currencies and blockchain technology"
Federal Reserve	September 2016	Chair declaration	Virtual Currencies / Distributed Ledgers	"…the Fed is trying to understand cryptocurrencies and blockchain[…] these technologies could have very significant implications for the payments system and the conduct of business."
US Congress	September 2016	Study group set-up	Virtual Currencies / Distributed Ledgers	The US Congress now has a caucus dedicated to bitcoin and blockchain
Federal Reserve	October 2016	Governor declaration	Distributed Ledgers	"…blockchain may represent the most significant development in many years in payments, clearing, and settlement."
Federal Reserve	December 2016	Report	Distributed Ledgers	"In the context of payments, DLT has the potential to provide new ways to transfer and record the ownership of digital assets; immutably and securely store information; provide for identity management; and other evolving operations through peer-to-peer networking, access to a distributed but common ledger among participants, and cryptography."

Source: BBVA Research

State level

New York

The New York Department of Financial Services (NYDFS) published BitLicense regulations for virtual currency businesses in June 2015. According to these regulations, firms engaged in “Virtual Currency Business Activity” that involves New York or a New York resident are required to apply for a BitLicense within 45 days of the effective date of the regulation. Applicants for a license are required to have, among other things, Anti-Money Laundering/Know Your Customer, Consumer Protection and Cybersecurity programs.

Vermont

Vermont decided to go beyond BitLicense schemes, giving legislative steps towards the utilization of blockchain technology for state registries, smart contracts and other applications, with the aim to become a “leader in the field”. An act relating to the promotion of economic development of 3 June 2015 commissions the writing of a report due January 15th 2016 with “...conclusions and recommendations about potential opportunities and risks of creating a presumption of validity for facts and electronic records using blockchain technology”.

The report published in January 2016 acknowledged that "blockchain is a reliable way of confirming the party submitting a record to the blockchain, the time and date of its submission, and the contents of the record at the time of submission". At the time of publication, however, it found that the cost and challenges of using blockchain technology outweighed its benefits but went on to encourage its legal recognition as a way to create a "first mover" advantage for the state.

In May 2016, Vermont adopted legislation to recognize blockchain data in the court system. The relevant provision is part of Bill H868 (An act relating to miscellaneous economic development provisions). In essence, the bill harmonizes blockchain data with Vermont's state law on the kinds of evidence admissible in court. Any document notarized using blockchain technology is to be considered legally admissible in court and have full legal bearing. According to Coindesk, the bill establishes that a document timestamped on a blockchain "shall be considered a record of regularly conducted business" when considered against the state's rules of evidence. The bill also establishes how the veracity of that certification can be challenged in court. However, Rep Bill Botzow, Chair of the Vermont House Committee on Commerce and Economic Development has emphasized that the bill is to apply "only to documents as opposed to financial transactions".

North Carolina

The North Carolina Money Transmitter Act is a Bitcoin-Friendly 'Virtual Currency Law’. The law updates the existing laws to define the term “virtual currency” and the activities that trigger licensure. Virtual currency miners and blockchain software providers will not require a license for multi-signature software, smart contract platforms, smart property, colored coins, and non-hosted, non-custodial wallets.

Delaware

Through its Delaware Block Initiative, launched in April, the state plans to engage technology vendors to help businesses and state agencies use blockchain technology to distribute, share, and save ledgers and contracts.

First up, the Delaware initiatives will work on using blockchain technology to store contracts and other essential corporate data on a distributed ledger, which will allow companies and agencies to store their documents in more than one location, keep them more secure and automate access by constituents, shareholders and employees. Other benefits include lower costs and longer documents retention. Typically, when documents are stored manually, the document is destroyed once the mandatory retention period passes. This will solve a big problem and could be very useful to government and public archives as well.

Indeed, the Delaware Public Archives will be among the first to use the distributed technology to archive and encrypt government archives later this year. Long pointed out that the use of blockchain means the documents are can be replicated in multiple locations, providing better disaster recovery and saving the cost of off-site physical storage.

California

California feels, rather than licensing virtual currency businesses, it should enroll them in a program to help the state learn more about the technology. Following this reasoning, California has been announced in August 2016 to launch the first US Virtual Currency Sandbox.

UK

The **FCA (Financial Conduct Authority)** inside its Project Innovate, "… is considering approving 'a small but significant number of firms' that use blockchain technology." In November 2016 they announced the first cohort of approved companies to enter in their Regulatory Sandbox Initiative: 9 out of 16 were blockchain-based firms.

International Bodies

The **FATF (Financial Action Task Force on Money Laundering)** published in June 2015 the "Guidance for a Risk-Based Approach to Virtual Currencies"[14] focused on the currencies themselves.

The **FSB (Financial Stability Board)** discussed and reviewed in March 2016, during a meeting in Tokyo covering its priorities in 2016, distributed ledger or blockchain technology.

The **OICV-IOSCO (International Organization of Securities Commissions)** is committed to analyse the impact of blockchain since it was included in its Securities Markets Risk Outlook 2016[15] published in February of that year.

The **BIS (Bank of International Settlements)** published a report in November 2015 stating that "digital currencies could reduce role of central banks".

The **IMF (International Monetary Fund)** published a report in January 2016 about "Virtual Currencies and Beyond: Initial Considerations."[16] More recently, in June 2016, they published in their web an article talking about DLTs as "The Internet of Trust"[17].

14: http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html
15: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD527.pdf

The **World Bank** published in June 2016 an article entitled "Blockchain technology: Redefining trust for a global, digital economy"[18].

The **WEF (World Economic Forum)** recently published a report on "The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services"[19]. In this report, they state that "Blockchain will become "beating heart" of the global financial system."

Central Banks

Although prior to 2016 central banks had practically not pronounced about blockchain technologies, apart from following the recommendation of the EBA to banks to "keep away" from virtual currencies, in 2016 movements have accelerated among them:

China: In January, news appear about China's Central Bank discussing digital currency launch. As of today, development of the e-yuan is supposed to be in process, but no further information has been given.

South Korea: In February, South Korea's Central Bank Encouraged to Explore Blockchain Tech

Russia: In February, Russia's Central Bank to Study Blockchain Tech. Further denied, but in June Digital Currency 'Still on the Agenda' at Russian Central Bank

Netherlands: In March, the Dutch Central Bank to Create Prototype Blockchain-Based Currency. In June, Dutch Central Bank Presents Results of Cryptocurrency Experiments with DNBcoin

France: In April 2016, the French Central Bank released a new report on financial stability in an era of digitization that multiple times touches on virtual currencies and blockchain technology. The report notes that the Banque de France is conducting its own research into the topic in cooperation with the Financial Stability Board (FSB). "Such [distributed ledger] models could replace the traditional operating mode clearinghouses based on aggregation and centralized clearing flows, affecting...the collateral management devices or rules for recording assets," the report states. At the same time, the Banque de France report authors argue that the technology is "still very largely in the experimental phase". The report said that future tests have to assess blockchain applications "in terms of safety, cost, [their] ability to handle quickly large volumes of transactions, or [the] economic interest to do without third trust for certain activities."

As an on-going initiative, the French government has passed a new ruling authorizing the use of distributed ledger technology for the issuance of mini-bonds and recording of trades. The new statute not only gives a clear definition of blockchain technology in French law, it also recognizes the technology as a recording tool that can be used for the transfer and authentication of ownership titles while providing legal validity to mini-bonds issued and traded via a blockchain infrastructure.

16: https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf
17: http://www.imf.org/external/pubs/ft/fandd/2016/06/adriano.htm
18: http://blogs.worldbank.org/ic4d/blockchain-technology-redefining-trust-global-digital-economy
19: http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf

Japan: In May 2016, a Bank of Japan Official stated: "The application of those technologies would also change the structure of the financial infrastructure that has been built around centralized ledgers managed by trusted third parties. Thus, central banks will and have to follow these issues closely and with great interest." Bank of Japan has announced its intention to issue its own cryptocurrency in 2017.

Canada: The Central Bank of Canada revealed in June 2016 that it was developing a digital version of the Canadian dollar based on blockchain technology, called CAD-coin. Bank of Montreal, CIBC, Royal Bank of Canada, Scotiabank and TD Bank, as well as banking consortium startup R3CEV, are said to be involved in the effort.

Participants would post cash to be held by the bank that would then be converted into CAD-coin. Verified counterparties would then process transactions, and the central bank would reserve the right to destroy CAD-coins as needed.

United Kingdom: In August, the Bank of England (BofE) indicated that it continues its research around central bank digital currencies (CBDC). A CBDC is a digital version of a national currency, which can theoretically be held in accounts owned by individuals or businesses at a central bank. Right now, only a small number of financial institutions are typically able to hold accounts at central banks, and everyone else must hold an account with one of those financial institutions. Two significant areas related to CBDCs that the BofE is researching are:

- Economic implications of a CBDC — specifically the possible reduction of the availability of credit. The ability to hold money at a central bank would likely lead people to move their money out of existing deposit accounts and into central bank accounts. That's because, unlike commercial banks, the central bank does not lend out deposits, so people might consider their deposits to be safer there. But this could lead to a reduction in deposit funding at commercial banks, which would negatively impact their ability to make loans, likely resulting in a significant reduction in the availability of credit. The risks this could pose are still being fully explored and understood.

- Technical feasibility of using blockchain technology to create a CBDC. Blockchain technology seems the most likely candidate for such a task, given its capability for creating multiple immutable ledgers and instantly recording transactions. But it is still very much experimental, and it's unclear whether the technology is the best way to achieve the necessary scale a CBDC would require. Also, the resilience and security of blockchain-based technology are still relative unknowns, as are the potential operational requirements.

Sweden: In November 2016, Sweden's central bank announced an initiative to analyze the possibility of introducing a digital currency to supplement cash in the country, given that people are increasingly cutting their use of coins and notes. The central bank has to assess in the coming years the technological, legal and policy implications of such electronic money. It also needs to be decided whether the money should be booked in accounts or some form of digitally transferable unit that doesn't need an underlying account structure, like cash.

Working Papers

2016

16/20 **Javier Sebastian Cermeño:** Blockchain in financial services: Regulatory landscape and future challenges for its commercial application.

16/19 **Javier Alonso, Alfonso Arellano, David Tuesta:** Factors that impact on pension fund investments in infrastructure under the current global financial regulation.

16/18 **Ángel de la Fuente:** La financiación regional en Alemania y en España: una perspectiva comparada.

16/17 **R. Doménech, J.R. García and C. Ulloa:** The Effects of Wage Flexibility on Activity and Employment in the Spanish Economy.

16/16 **Ángel de la Fuente:** La evolución de la financiación de las comunidades autónomas de régimen común, 2002-2014.

16/15 **Ángel de la Fuente:** La liquidación de 2014 del sistema de financiación de las comunidades autónomas de régimen común: Adenda.

16/14 **Alicia García-Herrero, Eric Girardin and Hermann González:** Analyzing the impact of monetary policy on financial markets in Chile.

16/13 **Ángel de la Fuente:** La liquidación de 2014 del sistema de financiación de las comunidades autónomas de régimen común.

16/12 **Kan Chen, Mario Crucini:** Trends and Cycles in Small Open Economies: Making The Case For A General Equilibrium Approach.

16/11 **José Félix Izquierdo de la Cruz:** Determinantes de los tipos de interés de las carteras de crédito en la Eurozona.

16/10 **Alfonso Ugarte Ruiz:** Long run and short run components in explanatory variables and differences in Panel Data estimators.

16/09 **Carlos Casanova, Alicia García-Herrero:** Africa's rising commodity export dependency on China.

16/08 **Ángel de la Fuente:** Las finanzas autonómicas en 2015 y entre 2003 y 2015.

16/07 **Ángel de la Fuente:** Series largas de algunos agregados demográficos regionales, 1950-2015.

16/06 **Ángel de la Fuente:** Series enlazadas de Contabilidad Regional para España, 1980-2014.

16/05 **Rafael Doménech, Juan Ramón García, Camilo Ulloa:** Los efectos de la flexibilidad salarial sobre el crecimiento y el empleo.

16/04 **Angel de la Fuente, Michael Thöne, Christian Kastrop:** Regional Financing in Germany and Spain: Comparative Reform Perspectives.

16/03 **Antonio Cortina, Santiago Fernández de Lis:** El modelo de negocio de los bancos españoles en América Latina.

16/02 **Javier Andrés, Ángel de la Fuente, Rafael Doménech:** Notas para una política fiscal en la salida de la crisis.

16/01 **Ángel de la Fuente:** Series enlazadas de PIB y otros agregados de Contabilidad Nacional para España, 1955-2014.

2015

15/33 **Shushanik Papanyan:** Digitization and Productivity: Where is the Growth? Measuring Cycles of Technological Progress.

15/32 **Alfonso Arellano, Noelia Cámara, David Tuesta:** Explaining the Gender Gap in Financial Literacy: the Role of Non-Cognitive Skills.

15/31 **Ángel de la Fuente:** Series enlazadas de Contabilidad Regional para España, 1980-2014. Parte II: Empleo asalariado, rentas del trabajo y salarios medios.

15/30 **Jingnan Cai, Alicia García-Herrero, Le Xia:** Regulatory arbitrage and window-dressing in the shadow banking activities: evidence from China's wealth management products.

15/29 **Javier Alonso, Alfonso Arellano:** Heterogeneity and diffusion in the digital economy: spain's case.

15/28 **Javier Alonso, Alfonso Arellano:** Heterogeneidad y difusión de la economía digital: el caso español.

15/27 **Angel de la Fuente**: Series enlazadas de Contabilidad Regional para España, 1980-2014.

15/26 **Carlos Casanova, le Xia and Romina Ferreira:** Measuring Latin America's export dependency on China.

15/25 **Nathaniel Karp, Boyd W. Nash-Stacey:** Embracing the Financially Excluded in the U.S.: A Multi-Dimensional Approach to Identifying Financial Inclusion Across MSAs and Between Cohorts.

15/24 **Alicia Garcia-Herrero, K.C. Fung:** Determinants of Trade in Parts and Components: An Empirical Analysis.

15/23 **Mariano Bosch, Angel Melguizo, Enith Ximena Peña, David Tuesta:** El ahorro en condiciones formales e informales.

15/22 **Antonio Villar:** Crisis, households' expenditure and family structure: The Palma ratio of the Spanish economy (2007-2014).

15/21 **Andrés Hernández, Bernardo Magnani, Cecilia Posadas, Jorge Redondo, Gonzalo Robles, Juan M. Ruiz y Enestor Dos Santos:** ¿Cuáles son los sectores con mayor potencial para aprovechar la Alianza del Pacífico?

15/20 **Gonzalo de Cadenas, Alicia Garcia-Herrero, Alvaro Ortiz and Tomasa Rodrigo:** An Empirical Assessment of Social Unrest Dynamics and State Response in Eurasian Countries. / *Published in Eurasian Journal of Social Sciences, 3(3), 2015, 1-29.*

15/19 **Mariano Bosch, Angel Melguizo, Enith Ximena Peña and David Tuesta:** Savings under formal and informal conditions.

15/18 **Alicia Garcia-Herrero, K.C. Fung, Jesus Seade:** Beyond Minerals: China-Latin American Trans-Pacific Supply Chain.

15/17 **Alicia Garcia-Herrero, Le Xia, Carlos Casanova:** Chinese outbound foreign direct investment: How much goes where after round-tripping and offshoring?

15/16 **Diego José Torres Torres:** Evaluando la capacidad predictiva del MIDAS para la Eurozona, Alemania, Francia, Italia y Portugal.

15/15 **Alicia Garcia-Herrero, Eric Girardin, Arnoldo Lopez-Marmolejo:** Mexico's monetary policy communication and money markets.

15/14 **Saidé Salazar, Carlos Serrano, Alma Martínez, Arnulfo Rodríguez**: Evaluation of the effects of the Free Trade Agreement between the European Union and Mexico (EU-MX FTA) on bilateral trade and investment.

15/13 **Saidé Salazar, Carlos Serrano, Alma Martínez, Arnulfo Rodríguez:** Evaluación de los efectos del Tratado de Libre Comercio entre la Unión Europea y México (TLCUEM) en el comercio bilateral y la inversión.

15/12 **Alicia Garcia-Herrero, Eric Girardin and Enestor Dos Santos:** Follow what I do, and also what I say: Monetary policy impact on Brazil's financial markets.

15/11 **Noelia Cámara, David Tuesta, Pablo Urbiola:** Extendiendo el acceso al sistema financiero formal: el modelo de negocio de los corresponsales bancarios.

15/10 **Noelia Cámara, David Tuesta, Pablo Urbiola:** Extending access to the formal financial system: the banking correspondent business model.

15/09 **Santiago Fernández de Lis, José Félix Izquierdo de la Cruz y Ana Rubio González:** Determinantes del tipo de interés del crédito a empresas en la Eurozona.

15/08 **Pau Rabanal and Juan F. Rubio-Ramírez:** Can International Macroeconomic Models Explain Low-Frequency Movements of Real Exchange Rates?.

15/07 **Ándel de la Fuente y Rafael Doménech:** El nivel educativo de la población en España y sus regiones: 1960-2011.

15/06 **Máximo Camacho and Jaime Martínez-Martín:** Monitoring the world business cycle. / *Published in Economic Modelling 51 (2015) 617–625.*

15/05 **Alicia García-Herrero and David Martínez Turégano:** Financial inclusion, rather than size, is the key to tackling income inequality.

15/04 **David Tuesta, Gloria Sorensen, Adriana Haring y Noelia Cámara:** Inclusión financiera y sus determinantes: el caso argentino.

15/03 **David Tuesta, Gloria Sorensen, Adriana Haring y Noelia Cámara:** Financial inclusion and its determinants: the case of Argentina.

15/02 **Álvaro Ortiz Vidal-Abarca and Alfonso Ugarte Ruiz:** Introducing a New Early Warning System Indicator (EWSI) of banking crises.

15/01 **Alfonso Ugarte Ruiz:** Understanding the dichotomy of financial development: credit deepening versus credit excess.

Click here to Access the Working Paper published

Spanish

and English

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