BANCO DE ESPAÑA
Eurosistema

ECONOMIC BULLETIN 4/2018
ANALYTICAL ARTICLES

16 October 2018

Distributed ledger technology (DLT): introduction

José Luis Romero Ugarte

Abstract

Distributed ledger technology is attracting the attention of the financial sector, both owing to its use in transactions with crypto-assets and to the proliferation of initiatives which have the potential to increase the efficiency, transparency, speed and resilience of processes underlying financial transactions. This article aims to introduce this technology, describing a series of basic issues surrounding it and attempting to identify opportunities and intrinsic limitations. Additionally, it addresses possible applications in the financial sector and outlines some of the main challenges which its use poses for the authorities.

Keywords: DLT, distributed ledgers, bitcoin, crypto-assets, cryptography, innovation, technology.

JEL codes: O31, O33.

DISTRIBUTED LEDGER TECHNOLOGY (DLT): INTRODUCTION

The author of this article is José Luis Romero Ugarte of the Directorate General Operations, Markets and Payment Systems.[1]

Introduction

Distributed ledger technology (DLT) refers to a database of which there are multiple identical copies distributed among several participants and which are updated in a synchronised manner by consensus of the parties. Although the best known application of this technology relates to crypto-assets (particularly the Bitcoin), in recent years a number of initiatives have proliferated in the financial sector, particularly in fields involving complex processes and numerous actors (e.g. securities trading and post-trading or foreign trade finance). In comparison with crypto-assets these initiatives show significant differences in terms of the complexity of the consensus mechanism or the characteristics of participants, which make them easier to implement. Thus, distributed ledgers are starting to be used as a tool that may contribute to reduce costs and increase the traceability, transparency and, in certain circumstances, speed of these processes.

However, distributed ledgers are not exempt from risks and limitations aside from those linked to the products for which they are being used (e.g. crypto-assets). At present, distributed ledgers are not sufficiently scalable, their soundness and resilience have not been sufficiently tested, the problem of participants' necessary trust in the system has not been fully solved and there is no interoperability between ledgers or with traditional infrastructures. Additionally, their use raises legal challenges (e.g. firmness of transactions), their governance is not always appropriate and, in certain cases, their operation entails a very high environmental cost.

The use of DLT by the financial sector also raises challenges for the authorities, since certain applications may lead to disintermediation of activities and affect the integrity of the financial system, so that it is not easy to clearly define responsibilities. Also, an adequate supervisory framework is lacking. Although the use of this technology is limited currently, it is advisable to analyse in depth its possibilities and implications in order to assess new projects as they arise and in view that the prospects are that it will continue to grow in the medium term.

What is a distributed ledger?

A distributed ledger is basically a decentralised, single database that is managed by several participants. It is a database of which there are multiple identical copies distributed among several participants and which are updated in a synchronised manner. An important difference between a distributed ledger and a "traditional" distributed database lies in the updating procedure: while in a traditional distributed database participants trust each other and cooperate to maintain data consistency, in a distributed ledger the parties do not trust each other completely (or there are conflicting interests) and, accordingly, a mechanism needs to be implemented to collectively verify ledgers before they are shared. In other words, the updates are not performed by a central authority, but by consensus among the parties, in accordance with a set of rules or procedures accepted by all.[2]

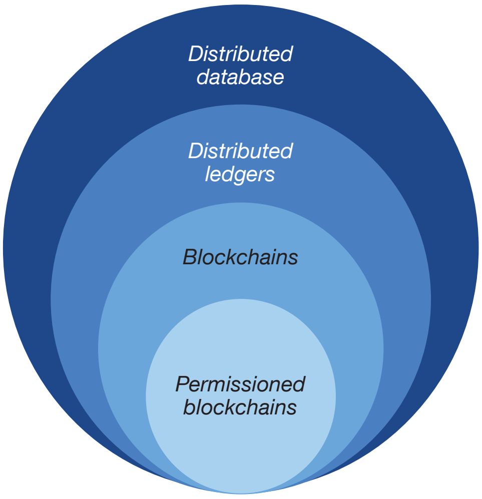
[1] The author thanks Juan Ayuso, Carlos Conesa, José Manuel Marqués, Ana Fernández, Sergio Gorjón and Esther Barruetabeña for their comments.

[2] These procedures enable all the parties to be sure that the data entries are not the result of a fraudulent transaction.

DISTRIBUTED LEDGERS AND BLOCKCHAINS ARE EXAMPLES OF DATABASES

FIGURE 1

Basically, a distributed ledger is a particular case of a distributed database which is characterised by its consensus-based validation process. Blockchain technology is an alternative for storing information in a distributed ledger, sequentially grouping transactions into blocks. There are two types of blockchain, depending on whether their access is open or restricted.



SOURCE: Global blockchain benchmarking study, Cambridge Centre for Alternative Finance.

Distributed ledgers are normally implemented by means of a blockchain or chain of blocks, which is a type of database (see Figure 1) where individual transactions are processed and stored in groups or blocks that are connected to each other in chronological order to create a chain. The integrity and security of the data stored in the chain are guaranteed by cryptography.

The first example of the practical application of the technology that we know of dates back to 2008, when one or several persons using the pseudonym Satoshi Nakamoto published a document[3] describing how the first “cryptocurrency” (the Bitcoin) functioned. The document provided a cryptographic solution, based on blockchain technology, to transfer this crypto-asset between parties that did not need to know each other and did not require a trusted third party. Since then, financial institutions, technological firms and developers, on one hand, and central banks and other authorities, on the other, have not ceased to experiment with this technology and its potential applications in an attempt to seek a secure, scalable system adapted to the financial sector’s needs.

Networks can be public or private, depending on how participants access them. The difference lies in whether or not there is a permission system to participate in the network, which also derives in differences in the consensus protocols used.

A public or non-restricted access network is completely open, anyone can participate. It requires an incentive-based system so participants will join the network to validate transactions. Bitcoin is the largest public network in production today. It uses remuneration in crypto-assets as an incentive to perform validations (validators receive bitcoins as a reward for the tasks involved, in this case, validation). Public networks have two main drawbacks: the first is that to achieve consensus, for example in the case of Bitcoin, potential validators are required to solve complex cryptographic proofs of work (mining)

[3] S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system,” October 2008.

which require a large amount of computational power. The second difficulty lies in how to maintain the privacy of transactions.

By contrast, in order to participate in a private network[4] it is necessary to receive an invitation and/or meet certain access requirements, and it is customary for participants to know each other. Private network operators may restrict the access of participants who are trusted to a certain degree and assign different roles to them,[5] which, in principle, would permit an easing of the requirements for validation of a ledger, improving scalability and limiting possible security problems. In transitioning from a public network to a private network, the anonymity and disintermediation of the network entail a cost in terms of efficiency. Consequently, most of the projects being developed by financial institutions are based on private networks.

How does DLT work?

DLT is basically the result of combining three already existing technologies (see Figure 2):

— *Peer-to-peer (P2P) networks:* In these models, each network participant (node) acts simultaneously as client and server, contributing and consuming resources. This technology became popular in 1999 with the launch of Napster, a software which basically allowed its users to share music.

— *Cryptography:* Specifically, asymmetric cryptography,[6] which allows for the secure exchange of information between two parties. It is used to authenticate the sender, to ensure the integrity of the message and, by means of encryption, to prevent third parties from accessing the information in the event they manage to intercept it.

— *Consensus algorithms:* They allow several participants, who may not know or trust each other, to reach an agreement to add new entries to the ledger. There are different methods to reach such consensus, i.e. to ensure that the ledgers of all the network participants are identical and that there is no fraud or duplication of information. The most popular one is “proof of work” (PoW), colloquially known as the mining process, which involves solving complex computational problems for the validation and creation of each new block in the chain. This mechanism, generalised by Bitcoin, entails consuming a large amount of energy in validating transactions (some estimates point to annual consumption of 71.12 TWh, similar to that of Chile, although there are no accurate data in this respect) and involves lengthy processing, which has led to the search for other more efficient mechanisms (e.g. “Proof of stake”).[7]

The storage, maintenance and updating of ledgers in a distributed ledger (see Figure 3) is the core of the technology. The responsibility for updating the ledgers is distributed among the nodes, who may be located in different environments, institutions or jurisdictions. Accordingly, changes in the ledger are often not updated simultaneously at all the nodes and there may be long wait times until all the versions are in sync.

[4] These networks are commonly known indistinctly as private, permissioned or closed networks.

[5] In some projects the assignment of roles enables the number of nodes which validate transactions to be limited.

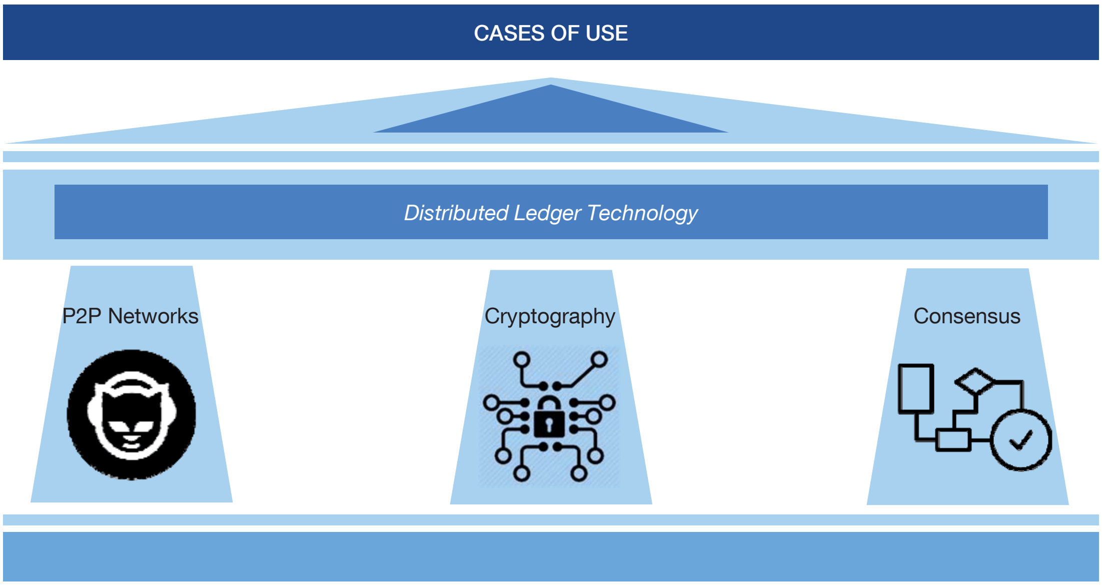
[6] Each user has a pair of keys, one public and one private. The public key may be given to anyone, who may use it to encrypt a message. That message can only be decrypted through the corresponding private key. Likewise, a message that has been encrypted with a private key can only be decrypted with the corresponding public key.

[7] Instead of mining, the validation is assigned to a specific node. The most common criterion used to select the node is the number of crypto-assets associated with each node in the network. Also, incentives and penalties can be set up to ensure that the node performs the validation appropriately.

DLT COMBINES THE THREE FOREGOING TECHNOLOGIES

FIGURE 2

DLT is basically the result of combining three already existing technologies: P2P networks, cryptography and consensus algorithms.



SOURCE: Prepared in-house.

Although each of the participants in DLT is a node, not all the nodes participating in the network necessarily carry out the same tasks. Thus, they may be mere points of access to the network for data entry, store ledgers, give their consent to transactions or act as hierarchically higher nodes whose approval is required for the definitive recording of a transaction. The different roles depend on the specific features of each network and each node may adopt more than one role at the same time.

One of the applications that seems most promising in connection with the use of DLT is the Smart Contracts application. In simple terms, these contracts are based on a code or IT protocol which facilitates the automated verification and performance of the underlying agreement, without the need for intermediaries. An illustrative example would be a coupon payment on a debt issue, where the purchaser is guaranteed that at the previously established maturity date the contract will self-execute and the related amount, calculated in accordance with the previously established conditions, will be transferred to the purchaser.

What is it for?

DLT technology has potential in many different areas, although especially in those in which there are many actors and a lack of trust between the parties.[8] Currently, the number of projects is proliferating, some of which are merely trials, although this does not necessarily mean that this technology is optimal for the processes involved.

The main stimulus to DLT technology has come from its applications as a medium for the exchange of crypto-assets, but its transforming potential is greater. In recent years, both the financial industry and certain authorities have launched many projects to experiment

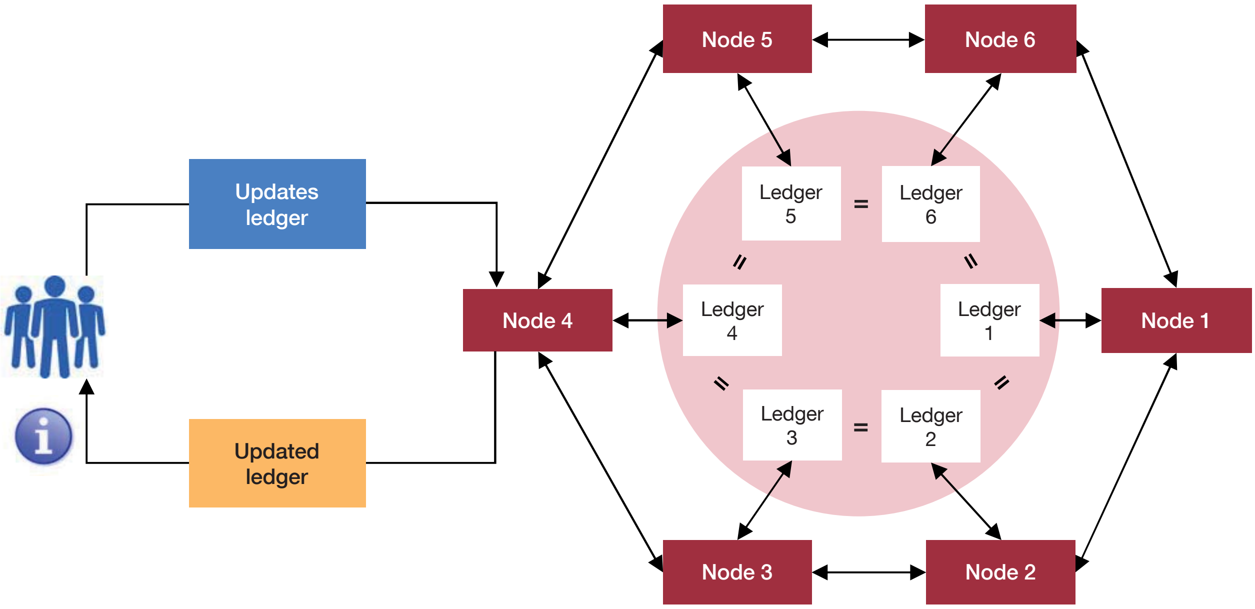
[8] A discussion of those cases in which it may currently make sense to use distributed ledger technology can be found in:
— Wüst and Gervais (2017).
— World Economic Forum (2018).

DLT UPDATING PROCESS

FIGURE 3

The following figure shows a very simple outline of the main steps required to update a distributed ledger:

a) To initiate the update, an agent uses cryptographic tools to digitally sign a transaction and sends it to the network through one of the nodes, requesting that it be processed.
b) Once the request is received, other nodes verify the applicant's identity and validate the transaction by means of the related consensus mechanism, confirming that the applicant has the credentials required to update the ledger (and a sufficient balance, if appropriate).
c) Once the transaction has been validated by the nodes, each of their ledgers are validated.



SOURCE: Prepared in-house.

with this technology in different areas. Some of the main uses currently being studied are presented below.

Some of the more promising projects are in the area of payments, specifically international fund transfers. This type of initiative increases the speed at which funds are made available, makes operations more transparent and significantly reduces their attendant costs. Some solutions enable funds to be exchanged rapidly and efficiently which, in addition to the advantages to users of instantaneously conducted transactions, entails a reduction in compensation and fraud risks, and reduces liquidity needs.

The most noteworthy projects in which central banks have participated, also in the payments area, have consisted in conceptual trials relating to interbank payments. These projects have identified strengths and weaknesses in the use of this technology for financial infrastructures and, although these experiences have been positively assessed, no overall advantages have been observed over current centralised interbank payment systems. However, there are alternatives that may be of interest in future, such as communication between different national payment systems or the introduction of another type of asset such as securities in the same ledgers, adding functionalities to the system.

In the area of securities trading and post-trading, DLT technology would enable a common digital database to be created, recording the ownership of securities and custody of assets, which would be shared among those with authorised access. Thus, there is potential to accelerate the settlement of financial transactions, reduce the number of intermediaries[9] and make the reconciliation process more efficient. Different securities market actors, both in the private sector and the authorities, have carried out projects to investigate the possibilities of this technology.

International trade is another area in which DLT technology could be applied, being characterised by the involvement of many actors as well as a large amount of documentation, so that processes tend to be complex and not always fully transparent, and can also be lengthy. A pilot study by a Spanish institution of the use of DLT in this area has highlighted the possibility of improving the efficiency of the process and ensuring it has traceability throughout. In addition, with the use of this technology, the transaction is validated and recorded transparently and securely for all parties.

DLT technology-based projects are also being pursued in the area of regulatory compliance (regtech). The aim of using this technology here is to optimise the way in which regulatory requirements (such as reporting obligations, transparency, risk management and control of money laundering and terrorist financing) are complied with. Potential improvements would include enhancing information quality, lowering the costs of processes, increasing flexibility and making outsourcing possible.

Finally, the spread of digitalisation in our society makes it necessary to strengthen the mechanisms to identify from a distance, precisely and efficiently those individuals acting in digital environments. That is to say, the question is how to ensure user trust in digital environments, which is important in all sectors, including finance. Some DLT technology-based projects offer precisely an identity management solution, upon which a digital ecosystem with diverse functionalities could be built.

Opportunities offered by adopting the technology

DLT technology has the potential to improve the design and, in particular, the efficiency of some markets, by:

— Eliminating messaging costs and reducing back-office costs, as there is less need for reconciliation between the parties when all the information is contained in one single shared ledger, with synchronised copies.

— Reducing transaction complexity and increasing traceability and transparency.

— Increasing the speed of processing in some cases or circumstances and, in consequence, improving liquidity management.

In particular, data traceability is a fundamental requirement for any ledger system, enabling any authorised entity to verify a transaction's history. Compared with other traditional systems, in which traceability is not always possible at all times and for all participants, this is one of the most important advantages of DLT technology. Moreover, traceability has implications for KYC (Know Your Customer) and for the prevention of money laundering and terrorist financing.

Traceability is linked to the immutability of transactions, which means that, once recorded, they cannot be modified. This characteristic is crucial to ensure data integrity and

[9] Including central counterparties, central securities depositories, brokers, custodians, clearing members and management and settlement entities.

security.[10] In combination, these two characteristics make the system transparent and secure for its participants, who may at any time access and consult the ledgers, in the confidence that they are reliable and cannot be altered, and in the certainty that other entities participating in the operations have exactly the same information.

In addition, DLT technology, depending on the type of ledger or transaction, allows different levels of privacy. Achieving a balance between privacy and transparency is not easy; the greater the information available to the validator, the lower the privacy of the network. By their very nature, processes based on DLT technology share more information than traditional centralised systems. Although in some models all nodes have a complete copy of the ledger and full transaction visibility, in financial sector applications, depending on participants' interests, access to the information may be restricted. This allows, in addition to the advantages of traceability and immutability of transactions, the possibility that each participant shares at any time only the information it wishes to share, either by means of encryption, the use of channels or other technologies. Although privacy is possible in a system or public network, there will be efficiency implications.

Limitations

DLT technology has certain limitations, in some instances on account of its immaturity. The limitations of the technology itself are identified below, as distinguished from those linked to the specific conditions of each use, such as in crypto-assets and the issuance of sovereign digital currency, which are not analysed in this article.

Currently, the scalability in the number of transactions and the speed with which they are registered are significant limitations. This is especially true in the case of public blockchain-based networks for three reasons: the number of transactions recorded in each block is usually limited, blocks have to be processed sequentially and the consensus mechanism is complex. Consequently, the system may become congested with a number of transactions waiting to be processed. The situation is better for private networks, but efficiency in this area is, as of today, well below the performance offered by other centralised systems.[11]

Doubts still remain as to the true robustness and resilience of DLT platforms, given that the technology has not yet been sufficiently tested. Moreover, there is still no appropriate regulatory framework providing sufficient legal coverage for the entries in distributed ledgers. For example, in the payments area, the time at which a transaction becomes final is not established. In future, solutions based on DLT technology will need to comply with the regulatory framework, which will vary according to the area of each application. This will be a challenge, given the distributed nature of the technology and because operations will probably be cross-border to maximise potential.

In the area of cyber security, firstly the distributed nature of the technology means that there are no unique points of compromise and resilience is improved, while the use of cryptography increases security. However there are other risks, such as losing the private key, which may provide attackers with full copies of databases, as well as the possibility

[10] In June 2016 the public network Ethereum suffered an attack involving the theft of crypto-assets with a value of some $70 million. Following a vote, the network participants agreed to reverse the fraud and return the funds. This solved the fraud, but called into question the immutability of DLT-based transactions.

[11] For example, the maximum number of transactions per second permitted by Bitcoin is seven, the Ethereum public network permits up to 23 and Quorum (a private protocol developed using the Ethereum code) boasts of the ability to deal with hundreds of transactions per second. The number of transactions per second permitted by card payment schemes is around 50,000.

that the concentration of network validation processes (i.e. “51% attacks”) may allow fraud through double expenditure or even transaction reversal.

Another weakness of the current state of this technology stems from the lack of interoperability of DLT ledgers, both among themselves (owing to the lack of standardisation) and with traditional infrastructures. Achieving this interoperability would entail costs that would have to be borne by the industry in a coordinated manner.

Governance systems are not always sufficiently efficient, transparent and responsible. Models vary from one platform to another, ranging from a fully decentralised system in which it is necessary to achieve consensus to make any change to system protocols or functions, traditionally used in public networks, to private networks with more centralised structures. The governance system chosen will be critical to ensure adequate risk management and, ultimately, to keep the system stable and secure.

Finally, the heavy average environmental cost arising from the use of proof-of-work systems (in public networks), which require high consumption of computing power and significant energy costs, must be included in this list, although there are other consensus algorithms, mainly in private networks, that do not have this limitation.[12]

Challenges for the authorities

DLT technology encompasses a variety of designs which are currently being experimented with. Each design has its own architecture, and it is possible to identify issues inherent to the technology in general and other features particular to each platform. In addition to the differences between public and private networks, one of the aspects that varies most across networks is the treatment of transaction privacy, an issue that is addressed differently in practically every project. All these aspects that are still to be defined pose new challenges for the authorities.

The architecture of DLT systems may lead to disintermediation of particular functions at certain entities, which could alter competition in financial markets, side-lining some traditional actors and, at the same time, permitting the entry of new participants currently not covered by the regulatory framework. This potential new scenario means that a fresh definition is needed for infrastructure responsibilities and actors in the provision of financial services.

Ensuring the security and integrity of transactions, in a broad sense, is fundamental to the stability of the financial system. In this respect, there is currently no supervisory or monitoring framework that allows DLT-based systems to be controlled by the authorities in the way that they can control critical infrastructures. At the same time, platform design and maintenance is not generally carried out by the user institution, so that there is a risk of loss of control over the infrastructure. This means it is difficult to foresee possible incidents, given the immaturity of the technology, and to take early action in the event of incidents.

In addition, from a central bank perspective, other aspects are also of concern, such as protection of bank service users, money laundering and terrorist financing, the security

[12] There are currently no reliable data on the electricity consumption of networks using this type of consensus algorithm, such as Bitcoin, but we can be sure that so-called “miners” face a very flexible cost structure. As compared with insignificant fixed costs, mainly relating to hardware, the variable costs of maintaining equipment (mainly refrigeration), and more specifically the consumption of electricity, are high and may discourage this activity. This is also the reason why most nodes are to be found in countries where electricity consumption is comparatively cheap. Estimating network energy consumption is extremely complex without the cooperation of miners, since it depends on variables such as the type of equipment used.

and efficiency of payment systems, the integrity of the financial system and the exercise of supervision and oversight. Given the cross-cutting nature of the technology, the importance of which transcends financial services and which may have applications in other sectors of the economy and society, the European Commission has launched the EU Blockchain Observatory and Forum, one of the measures presented in the "FinTech Action plan: For a more competitive and innovative European financial sector". Launched in February 2018, for a period of two years, it will attempt, inter alia, to develop the governance and standards for the technology.

Under the auspices of the Eurosystem, a network of central bank experts has been created, in which the Banco de España is participating. The objective is to share knowledge and information and to achieve a better understanding of the opportunities and challenges raised by the use of DLT technology, focusing in particular on the area of payments and market infrastructures.

Conclusions

DLT technology emerged as a combination of various prior innovations and has been popularised by the appearance of Bitcoin. However, it is important to highlight that Bitcoin is only one particular application of this technology, the potential scope of which is much broader.

Given its intrinsic characteristics, the areas in which this technology seems to have the greatest chances of success are those in which shared ledgers are used by many participants (or in which their use may be efficient), and more than one participant may modify such ledgers, but there is a degree of mistrust among them or they have conflicting interests.

As of today, the technology is still incipient as regards its effective implementation in productive processes relating to the provision of financial services, which means that greater experimentation by the industry is advisable (and can be expected). At the same time, the characteristics of DLT, its potential and its possible implications for the financial system mean that the authorities should continuously monitor the developments in the market.

16.10.2018.

REFERENCES

BANK FOR INTERNATIONAL SETTLEMENTS (2017). Distributed ledger technology in payment, clearing and settlement.

CITI GLOBAL PERSPECTIVES AND SOLUTIONS (2018). Bank of the future: The ABCs of Digital Disruption in Finance.

FINANCIAL INDUSTRY REGULATORY AUTHORITY (2017). Report on Distributed Ledger Technology.

HILEMAN, G. and M. RAUCHS (2017). Global Blockchain Benchmarking Study, Cambridge Centre for Alternative Finance.

MILLS, D., K. WANG, B. MALONE, A. RAVI, J. MARQUARDT, C. CHEN, A. BADEV, T. BREZINSKI, L. FAHY, K. LIAO, V. KARGENIAN, M. ELLITHORPE, W. NG and M. BAIRD (2017). "Distributed ledger technology in payments, clearing and settlement", Journal of Financial Market Infrastructures, 6(2/3), pp. 207–249.

NAKAMOTO, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

WORLD BANK GROUP (2017). Distributed Ledger Technology (DLT) and Blockchain.

WORLD ECONOMIC FORUM (2018). Blockchain Beyond the Hype. A Practical Framework for Business Leaders.

WÜST, K. and A. GERVAIS (2017). Do you need a Blockchain?, Department of Computer Science, ETH Zurich, Switzerland.