Briefing
November 2016

European Parliament

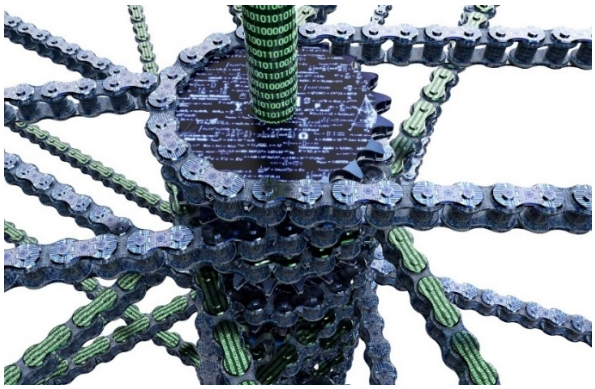
Distributed ledger technology and financial markets

SUMMARY

Distributed ledger technology (and one of its sub-categories, 'blockchain' technology) has attracted interest from financial market participants, venture capitalists and regulators alike, with regard to its potential application in certain post-trading (mainly clearing and settlement) activities in financial markets.

Potential benefits include increased processing speeds and easier recording of ownership and safekeeping of assets, which could result in significant cost benefits as well as greater security. These stem from the fact that there are fewer contract ambiguities, reduced counterparty risk and easier collection, consolidation and sharing of data for reporting, risk management and supervisory purposes.

However, academics and regulators have also identified several operational, governance, privacy and legal concerns and potential risks that should be addressed adequately before this technology is used for supporting infrastructure as critical as that underpinning financial services. In this context, the European Securities and Markets Authority (ESMA) has launched a consultation on the application of distributed ledger technology to securities markets. The European Parliament, in its 26 May 2016 resolution on virtual currencies, called on the European Commission to set up a horizontal task force for distributed ledger technologies, made up of technical and regulatory experts, who should aim to provide the necessary technical and regulatory expertise across the various sectors of pertinent distributed ledger applications.



In this briefing:

EPRS | European Parliamentary Research Service
Author: Angelos Delivorias
Members' Research Service
PE 593.565

EN

Glossary

Distributed ledgers constitute databases spread across multiple sites, countries or institutions, which are typically accessible by anyone. Records of transactions are stored one after the other in a continuous ledger, rather than sorted into event-specific or thematic blocks, but they can only be added once the participants reach a quorum. A ledger is 'un-permissioned', if it has no single owner and the process is open to everyone (as in the case of Bitcoin). The integrity of the ledger is maintained through consensus from the participants about its state. In contrast, if participants in the process are preselected, the ledger is permissioned. Here, the consensus process is simpler and carried out by third parties, usually government departments or banks. That is also what makes the permissioned ledger process usually faster than the un-permissioned one.

Operational risk is the risk of losses stemming from inadequate or failed internal processes, people and systems, or from external events.

Smart contracts are contracts whose terms are recorded in a computer language. These contracts can be automatically executed by a computing system, such as a suitable distributed-ledger system. Potential benefits include low contracting, enforcement, and compliance costs, while potential risks include a reliance on the computing system that executes the contract.

Source: 'Distributed Ledger Technology: beyond block chain', a report by the UK government chief scientific adviser; website of the European Banking Authority.

Introduction

The blockchain is a type of database that takes a number of records and assembles them in a block, which is then 'chained' to the next block using a cryptographic signature. This allows them to be used like a traditional ledger, which can be shared and corroborated by anyone with the appropriate permissions. Until recently, the most widely known application of this technology was in the public ledgers of transactions underpinning virtual currencies, such as Bitcoin. Recently, however, the idea that the use of this and similar methodologies belonging to the wider group of 'distributed ledger technologies' could be extended to traditional financial services,[1] has been gaining ground. Some market participants and market infrastructure providers have started working on initiatives to leverage this technology, and industry members think that it could bring them significant benefits.[2] Recent investment trends have duly reflected these developments, with venture capital investment in the technology reaching almost US$1 billion. This briefing attempts to provide an introduction to the discussion.[3]

Financial market infrastructure and distributed ledger technology

A ledger is a set of accounts. Ledgers can be maintained by a single company (for instance, a bank), or can be 'distributed', thus forming a database that can be spread across multiple sites, countries or institutions. If the records of this distributed database are sorted into blocks, the database is called a blockchain. If the records are stored one after the other in a continuous ledger, the database is called a distributed ledger, although it must be noted that the terms are frequently used interchangeably by the press.

This feature (maintenance by a shared network of participants acting as network nodes, rather than by a centralised entity), as well as the extensive use of cryptography to store assets and validate transactions, set those databases apart from 'traditional' ledgers.[4] The fact that users can modify records in this 'shared' ledger without needing to use a central system for validation gave rise to the idea that this technology could potentially be used

for creating ledgers that settle trades for any given set of assets and their holders in the financial markets.

Area of application in financial markets

Both the European Securities and Markets Authority (ESMA) and authors from the European Central Bank (ECB) share the view that distributed ledger technology will, at least initially, be explored primarily for certain post-trading activities – **clearing, settlement, custody and asset servicing** – which are performed after the execution of a trade by financial market infrastructures.

Clearing is the process of transmitting, reconciling and, in some cases, confirming transfer orders. The process can include the netting of orders (offsetting of mutual obligations) and the establishment of final positions. The risk of failed trades is reduced by interposing a central counterparty (CCP) between the dealers of either party.

Settlement activities deal with the effective transfer of ownership of securities from a seller to a buyer and the respective transfer of cash from a buyer to a seller. Upon settlement, the securities purchaser obtains the proprietary rights to the security. Originally held in physical form, certificates were first 'immobilised' and later 'dematerialised'. Nowadays mainly existing in electronic form, they are held indirectly through a book-entry system run by a custodian, typically a Central Securities Depository (CSD), which transfers ownership in its records upon evidence of payment. Risk is reduced through settlement finality, which ensures that the insolvency of one participant does not result in the unwinding of transactions between the other participants in a settlement system.

Possible benefits of distributed ledger technology for securities markets

Usually the settlement of equities, bonds, mutual funds and municipal securities in the US takes place within three business days after the transaction date ('T+3'), while in Europe the standard is 'T+2'. ESMA notes that distributed ledger technology could possibly **speed the clearing and settlement** of cash financial transactions by making the reconciliation process faster and more efficient. Another benefit is that it could **facilitate the recording of ownership** of a variety of securities and the **safekeeping of assets**, among other things, by promoting a unique reference database and reducing the possible ambiguity of contract terms. Furthermore, it could **reduce the uncertainty** related to contract terms and help **render the processing of corporate actions more automated** through the use of *smart contracts*. Finally, it could facilitate the **collection, consolidation and sharing of data for reporting, risk management and supervisory purposes**, by enlarging the scope of information available from a single source and by making access to this information easier and faster. ESMA notes that the use of this technology could potentially reduce **counterparty risk**, at least with regard to spot securities transactions,[5] by shortening the period a party is exposed to the risk of default by the other party. The resulting reduced need for collateral and the capacity to speed collateral movements would increase **market collateral availability**.

Other benefits identified come in the form of **high level of availability** (in an area where processes are usually organised in batches), **high security** (grounded on the distributed nature of the ledger and the use of cryptography and consensus to secure and validate transactions), and a **general reduction of costs** (as a result of decreased transaction costs, streamlined middle and back-office processes, reduced maintenance costs at company level and diminished need for business continuity plans).[6]

Key issues and possible risks

Operational issues

By examining issues encountered with Bitcoin, Angela Walch questions whether the technology is robust enough to serve as the foundation of major payment, settlement, clearing, or trading systems. Indeed, the **software can have 'bugs'** (such as 'Heartbleed'), which are 'low-likelihood, high-consequence threats'. It **may be vulnerable to attacks** (such as a '51 % attack' or a 'Distributed Denial of Service Attack') and it is **ever-changing through new releases** (which can result in unacceptable 'forks' in the code resulting from uneven updating on behalf of participants, technical issues or fundamental disagreements stemming from wider policy choices). Last, but not least, **few people understand how it works**, which, as the latest financial crisis has demonstrated, might result in important systemic risks.[7]

Similarly, ESMA has voiced concerns with regard to operational risks that relate to: the **scalability** of the technology (what has been achieved for targeted activities might be difficult to replicate on a wider scale involving a broad range of instruments and participants); its **interoperability** with the existing systems (that is, market infrastructure) and across the different networks (that is, separate ledgers used for different types of assets); possible **legal and technical challenges** arising from the need to settle in central bank money (in order to achieve full 'Delivery-versus-Payment'); the **recourse** (that is, mistake correction) **mechanisms** and timeframes; the **use of the system** (currently accounting on a 'gross' basis, which is good for cash 'spot' transactions) **to record derivative transactions** (for which position margins and collateral requirements are computed on a net basis); and to difficulties in using the system for **margin finance and short selling** (because the possession of assets is a prerequisite for transacting).

Governance issues

According to Andrea Pinna and Wiebe Ruttenberg, the adoption of distributed ledger technology for use in the post-trade phase of securities transactions will face the same issues as the current post-trade set-up is experiencing, that is, the need for common technical standards and business rules. Similarly, ESMA is of the view that, given distributed ledger technology will be *permissioned*, there will be the need for rules[8] to approve or reject authorised participants and to govern the interactions between them. Angela Walch notes that risk can emerge from the open-source nature of the technology – especially if there is no authority with the responsibility to keep the software/system operational – because no one may be implementing necessary fixes,[9] because the management of the code (and therefore the infrastructure) might be shaped by conflicts of interest and because consensus on changes might not be achieved, leading to the aforementioned forks in the network. Furthermore, there will need to be clear rules for developers tasked with creating the framework, as conflicts of interest may emerge.[10]

Privacy issues

ESMA notes that by design, in a distributed ledger environment, the information recorded on the ledgers (that is, the history of the transactions and the balance of cash and assets held on accounts) is made public to the participants in the network, or at least to permissioned participants. This raises the question of how to strike a **balance** between the **public nature** of the information recorded by using the technology, and the **need for anonymity** or privacy the participants might have with regard to part of the information provided.

Regulatory and legal issues

Differences in securities and company laws across the EU may impede the deployment of distributed ledger technology in securities markets. Furthermore, **legal issues**, such as the legality and enforceability of the records kept on the blockchain, also need to be considered carefully. Finally, **supervising** a distributed ledger 'network' might be substantially more complex than supervising central market infrastructures.[11]

Possible risks

While in principle distributed ledger technology should enhance the traceability of transactions and transparency in securities markets, the complex encryption techniques used could add another **layer of complexity** to securities markets, at least in the short term. Furthermore, **migration** to the new distributed ledger environment carries risks, just like every migration to a new system. In addition, the distributed nature of the ledger is a double-edged sword: while it does increase security, ESMA notes that, if nevertheless someone were to hack the system, they could obtain **access to all the information**, and not only the data stored at the point of attack. Furthermore, given that the protocols used by different distributed ledger networks tend to be similar, the **hacking of one network may jeopardise the security of many others**. In addition, private/public keys might be lost or stolen and then **used fraudulently to record fictitious transactions**. Similarly, in the absence of adequate checks, distributed ledger technology could be exposed to the **risk of money laundering and terrorist-financing activities**, notably because the use of public/private keys could make it easier to conceal identities and to hide the history of transactions. Finally, the use of distributed ledger technology could contribute to **herding behaviour** and **increase market volatility** in times of stress to the financial system.

State of the market

Despite the industry's acute interest and the fact that investment, at the end of 2016, has neared US$1 billion, distributed ledger technology is still in its infancy: there is no legal standard for the transfer of property rights, and the technology does not yet permit netting of transactions or ex-post corrections. Furthermore, while banks can see benefits, they have not yet committed to a system where competitors can potentially access each other's data and thus gather intelligence regarding each other's transactions. Finally, a broad range of legal implications and technological issues remain a challenge.

Applicable (current) EU regulatory framework

Clearing activities

Within the EU, **clearing** activities are governed by the European Market Infrastructure Regulation (**EMIR**), which deals with OTC derivatives, central counterparties and trade repositories, and the Markets in Financial Instruments Directive and Regulation (**MiFID/MiFIR**), which govern the provision of investment services in financial instruments by banks and investment firms, as well as the operation of traditional stock exchanges and alternative trading venues. ESMA envisions three situations: (i) the clearing of OTC derivatives in a distributed ledger technology environment, where the parties to a distributed ledger network would need to comply with EMIR,[12] (ii) the clearing of exchange-traded derivatives in a distributed ledger environment, where, according to Article 29 MIFIR, the parties would need to clear their transactions through a CCP (therefore still needing to comply with EMIR), and (iii) the clearing of transactions of other types of assets, such as securities lending and repurchase agreements, in a distributed ledger environment, in which case the applicable framework would depend on whether

or not those other types of assets are cleared by a CCP (if yes, the CCP would need to comply with EMIR rules, and if not, national rules would still apply).

Settlement activities

Settlement activities are primarily governed by the Settlement Finality Directive (**SFD**), which aims to reduce the systemic risk associated with participation in payment and securities settlement systems, in particular the risk linked to the insolvency of a participant, and by the Central Securities Depositories Regulation (**CSDR**), which aims to harmonise certain aspects of the settlement cycle and settlement discipline, and introduces common rules for central securities depositories.

ESMA envisions two possible situations: the settlement of securities transactions by (i) a distributed ledger network that is not designated as a securities-settlement system by its home Member State, or (ii) a distributed-ledger network that is designated as a securities-settlement system.

In the first case, SFD would not apply and the network would not qualify as a CSD. Two possibilities could emerge: that the distributed ledger network does not act as a settlement internaliser under CSDR, in which case it would not be subject to the reporting requirements under CSDR,[13] or that it does act as a settlement internaliser, in which case it would have to comply with the reporting obligations laid out in Article 9 CSDR. In the latter case, both the SFD requirements (for instance, Article 2) and CSDR requirements (for instance, Article 18) would apply.

Safekeeping and record-keeping of ownership of securities and of rights attached to securities (including asset servicing)

Contrary to clearing and settlement, the legislation applicable to securities and the rights attached to securities is not harmonised at EU level but is defined at national level in many cases. ESMA highlighted two scenarios: (i) record-keeping of ownership happens at issuer level (in which case the rules will depend on each country's national corporate law), and (ii) record-keeping of ownership happens at the investor level (in which case the rules will vary across several sectoral pieces of legislation, such as MiFID, the Undertakings for the Collective Investment in Transferable Securities (**UCITS**) Directive, which deals with the coordination of laws, regulations and administrative provisions relating to those undertakings, or the Alternative Investment Fund Managers Directive (**AIFMD**), which aims to increase the transparency of those funds, strengthen investor protection and provide supervisors with the data and tools necessary to monitor and respond to stability risks they may create).

Regulatory reporting activities

Several pieces of EU legislation, such as MiFID, EMIR and SFTR, have introduced an obligation for market participants to report to national competent authorities or third parties such as trade repositories. ESMA points out that, if market participants choose to set up a distributed-ledger network to provide the same exact functions as trade repositories, they will need to have a trade repository that complies with EMIR.

European Parliament position

On 26 May 2016, the European Parliament adopted a resolution on virtual currencies. The resolution recognises that virtual currencies and blockchain technologies have the potential to contribute positively to citizens' welfare and economic development, but stresses that such technologies entail risks which need to be addressed appropriately so as to enhance their trustworthiness. It suggests that addressing these risks will require

the development of a sound legal framework that keeps up with innovation, but notes that if a regulation is adopted at a very early stage, it may not be well adapted to a state of affairs which is still in flux, and thus may convey the wrong message to the public about the advantages or the security of such technologies. It notes furthermore that key pieces of EU legislation, such as EMIR, CSDR, SFD, MiFID/MiFIR, UCITs and AIFMD, could provide a regulatory framework in line with the activities carried out, irrespective of the underlying technology, while observing that in time, more tailor-made legislation might be needed.

Furthermore, the resolution calls for the creation of a 'horizontal Task Force DLT' led by the Commission and consisting of technical and regulatory experts, whose remit would be to:

- provide the necessary expertise across the various sectors of pertinent distributed ledger applications;
- bring together stakeholders and support the relevant public actors at EU and Member State level in their efforts to monitor distributed ledger technology use at the European level and globally;
- foster awareness, and analyse the benefits and risks – including to end-users – of distributed ledger applications in order to make best use of their potential;
- support a timely, well-informed and proportionate response to the new opportunities and challenges arising with the introduction of significant distributed ledger applications; and
- develop stress tests for all relevant aspects of such schemes that reach a level of use that would make them systemically important for stability.

Main references and further reading

Andrea Pinna and Wiebe Ruttenberg, 'Distributed ledger technologies in securities post-trading – Revolution or evolution?', ECB Occasional Paper, April 2016.

Dong He et al., 'Virtual currencies and beyond', International Monetary Fund, January 2016.

ESMA Discussion Paper, 'The Distributed Ledger Technology Applied to Securities Markets', 2 June 2016.

European Parliament resolution of 26 May 2016 on virtual currencies, 2016/2007(INI).

Joanna Diane Caytas, 'Developing Blockchain Real-Time Clearing and Settlement in the EU, US, and Globally', 22 June 2016.

Mark Kalderon, Ferdisha Snagg and Claire Harrop, 'Distributed ledgers: a future in financial services?', Journal of International Banking Law and Regulation, 2016, 31(5), pp 243-248.

Oxera Economics, 'The debate about blockchain: unclear and unsettled?', August 2016.

UK Government office for Science, 'Distributed Ledger Technology: beyond block chain', 2016.

Endnotes

1 The website http://www.blockchaintechnologies.com gives the examples of Ripple, MultiChain or HyperLedger.

2 Such as Nasdaq or the Australian Securities Exchange.

3 Therefore it will deal with the application of the technology in securities markets (that is, mainly in post-trading). Issues related to the payments aspect of virtual currencies have been treated in other EPRS briefings – see for example 'Bitcoin: Market, economics and regulation by Marcin Szczepanski, and 'Virtual currencies: Challenges following their introduction' by Christian Scheinert.

4 That is, computer-based encryption techniques such as public/private keys and hash functions.

5 In 'spot' transactions, a single settlement extinguishes the obligations of the respective parties at once. On the contrary, in derivatives transactions, obligations remain through the entire life of the contract, which implies that there is the need to mitigate the counterparty risk throughout the life of the instrument. For this reason, ESMA is of

the view that the distributed ledger technology is unlikely to eliminate the counterparty risk from derivatives transactions and hence the benefits of CCP clearing for derivative instruments are likely to remain unchanged.

[6] This implies that there is no single point of (cyber) attack.

[7] Although the author is careful to also note the viewpoint of bitcoin proponents, who counter that such an attack would be highly unlikely for various reasons, as explained in the paper.

[8] With regard to minimum capital, conduct of business rules or risk management processes.

[9] No authority might have the necessary legitimacy to do so, even if it wants to step in.

[10] Walch gives an example with Bitcoin developers to show that a code developer might prioritise their employer's interests over the interests of the community as a whole.

[11] Especially if one considers that different nodes might be established in different jurisdictions and be subject to different privacy and insolvency rules, as well as to other divergent requirements.

[12] Specifically, they would need to comply with Article 5 in case the OTC derivative transactions are subject to the clearing obligation by CCPs, and with Articles 11–15, in case those OTC transactions are not subject to the clearing obligation.

[13] See Article 2, point 11.

Disclaimer and Copyright

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)