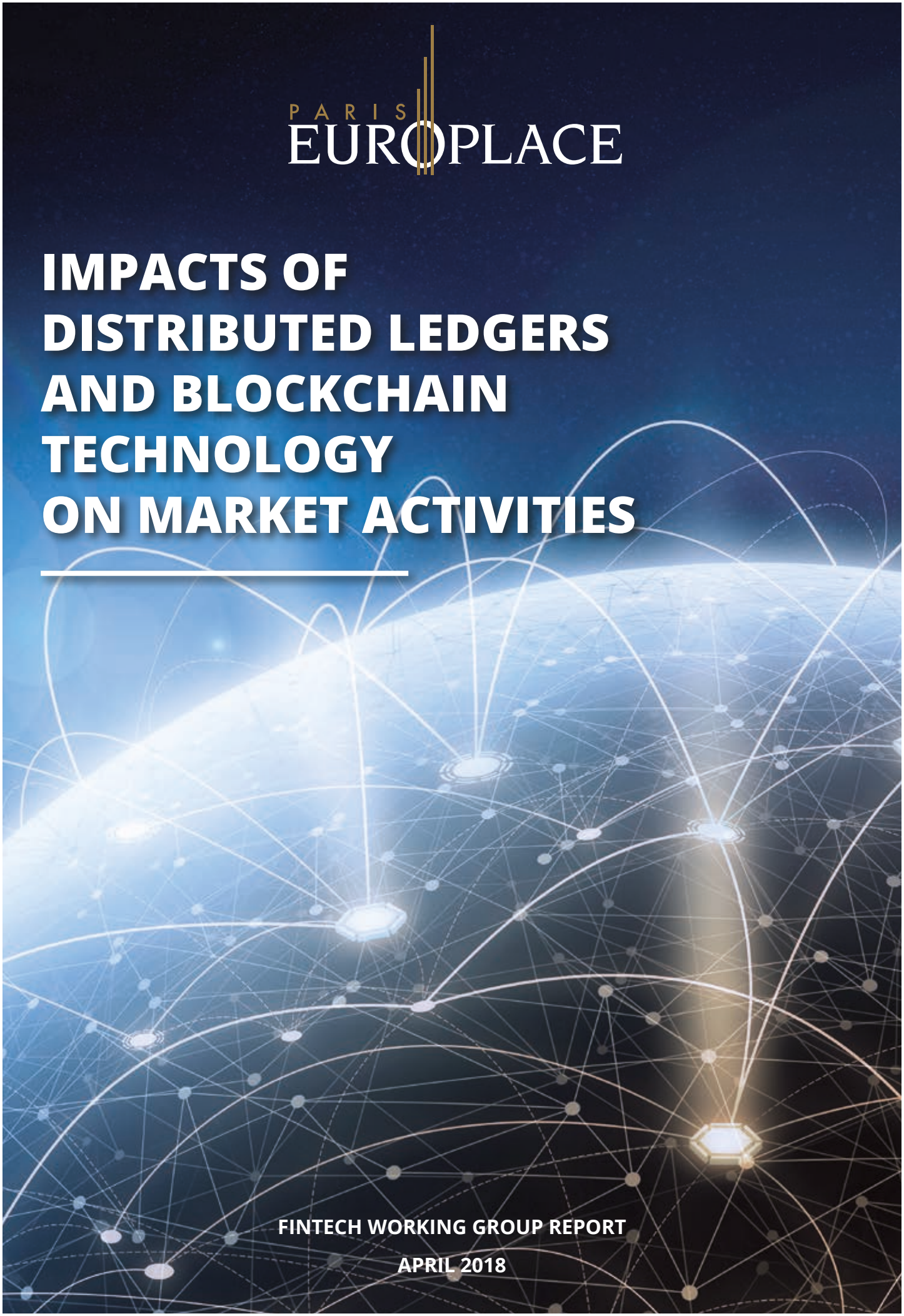
PARIS EUROPLACE

IMPACTS OF DISTRIBUTED LEDGERS AND BLOCKCHAIN TECHNOLOGY ON MARKET ACTIVITIES



FINTECH WORKING GROUP REPORT

APRIL 2018

EXECUTIVE SUMMARY

The Paris EUROPLACE Blockchain working group took on the task of studying the effects of blockchain technology on two financial activities: asset management and the activities of depository / custody account keeping. This decision was prompted by the importance of the consequences that this new technology may have on these activities, particularly as France hosts important international players in these areas. Additionally, the consultation launched concomitantly by the French Treasury on the adaptation of French law to blockchain technology in the area of securities law assured this working group of the pertinence of their decision.

The present report's scope surpasses that of the French domestic context and the consultation launched by the Treasury on securities law. It is worth noting that France is one of the first countries in the world to legislate on the use of blockchain in post-trading activities and securities law. The adaptation of French law concerning this new technology has not resulted in a new branch of law, but rather has expanded general principles concerning civil and commercial law, in turn allowing for the majority of legal questions around blockchain to be resolved. French law has in fact adapted to this technology, notably with regards to the notion of 'securities trading account', the redefinition of which was required.

More fundamentally, the working group is of the opinion that the object of regulation ought not to be a technology or an infrastructure in itself, but rather their uses.

With particular focus on asset management, the most effective use of blockchain technology is paving the way for a fundamental change in the form of units and shares in collective investment funds in France, changing from bearer securities to registered securities. This is not without consequences for securities issuers which are as a result required to carry out a considerable amount of verifications themselves and to take on direct responsibility for administrative and fiscal procedures.

As far as securities law is concerned, this analysis concludes that the adaptation of the existing law on unlisted securities is sufficient to allow for the use of blockchain technology.

CONTENTS

INTRODUCTION

THE ORIGINS OF BLOCKCHAIN

For nearly ten years, blockchain has experienced a booming success. It is on everybody's lips, in particular in the banking and finance world where it finds its source. A plethora of articles, studies, speeches and debates are themed around the 'Blockchain revolution', a tide on par with the democratisation of the internet which changed the world in the early nineties. However, beyond the intellectual excitement, there is still few concrete realisations with regards blockchain - is it just a fad, making promises it cannot keep?

To understand this technology, we must first understand where it came from. Blockchain was not in fact created for its own intents and purposes - originally, it was only an aspect of Bitcoin protocol, ensuring the secure transfer of the cryptocurrency. Renowned worldwide, Bitcoin came into being in early 2009, for the purposes of autonomy, as it was designed to be managed by members of the Bitcoin 'community'. Entirely decentralised, it operates according to a complex system of mathematical algorithms which, from the beginning, governed its methods of transfer, rules of consensus, and even the moment when new Bitcoins were created.

All Bitcoin transfers must therefore adhere to the established rules of peer consensus. This consensus can only be reached if the members of the community approve the transfer with respect to a decentralised Bitcoin ledger held by each member of the community. This is when blockchain comes in.

It is important to define right from the beginning that the 'libertine' essence of Bitcoin was the fundamental precursor to the creation of blockchain. In fact, it is thanks to blockchain that users of this cryptocurrency were able to trade safely, without the need for a regulatory intermediary, which was seen as a threat to freedom.

Bitcoin's underlying technology was rapidly adopted by various sectors of everyday life. Blockchain quickly proved itself to be an extremely effective certification tool which, thanks to mutual trust between members of its community, allowed for a far more efficient system of decision-making. Reputed for its immunity to fraud, blockchain assures its users of the indubitable credibility of the information it contains. In a time of massive online exchange, blockchain provided a vital advantage in the never-ending challenges of cyber security.

THE RELATIONSHIP BETWEEN FINTECH AND BLOCKCHAIN

Blockchain's current notoriety is largely thanks to the work of FinTech companies, which put a range of technological innovations, including blockchain, at the service of banking and finance institutions.

In a public consultation called 'FinTech: a more competitive and innovative European financial sector', the European Commission highlights the innovative potential of FinTech companies:

> *'While technological innovation in finance is not new, investment in technology and the pace of innovation have increased significantly in recent years. Among other things, technological innovation is driving social networks, artificial intelligence, machine learning, mobile applications, distributed ledger technology (DLT[1], cloud computing and big data analytics. They give rise to new services and business models by established financial institutions, technology companies and new market entrants. FinTech involves the entire financial sector, including front, middle and back-office activities, as well as services for both retail and wholesale markets.'*

In this consultation, the European Commission (EC) underscores the importance of technological neutrality - that is, the guarantee that all activities of a certain category be subject to the same regulations, regardless of the technological means of deployment of the service - in order to foster innovation and maintain healthy competition.

[1] *Order n° 2016-520 of 28 April 2016 concerning savings bonds.*

The consultation will be foundational for future developments in the EC's policies with regards to technological innovation in financial services.

INITIATIVES LAUNCHED BY REGULATORS AND MARKET STAKEHOLDERS

Several initiatives relating to the use of blockchain have come to light in the French banking and finance sectors, illustrating France's capacity to approach a wide range of subjects.

As soon as July 2016, the Banque de France, joined by, among others, the start-up Labo Blockchain and the Caisse de Depots et Consignations, launched an experiment involving blockchain and one of the standard references that it manages, the SEPA Creditor Identifier. A test blockchain infrastructure was set up for the purposes of this experiment to identify the primary technical and operational difficulties of this technology.

Similarly, a consortium of financial entities was assembled to develop a blockchain infrastructure for SME back offices. This consortium was made up of Euronext, BNP Paribas Securities Services, the Caisse de Depots et Consignations, Euroclear, S2iEM and Société Générale and supported by Paris EUROPLACE. This pan-European initiative's goal was to offer SMEs an effective and cost-efficient solution to post-trading processes.

The Caisse de Depots et Consignations also launched its first test of blockchain, with the initiative LaBChain, focusing on digital identity and the challenges of client ID verification - 'know your customer' (KYC).

THE INVOLVEMENT OF FRENCH REGULATORY AUTHORITIES

French regulatory authorities acted as precursor in the area of financial innovation, as demonstrated by the order of 28 April 2016 regarding 'bons de caisse'1, establishing a new hybrid security called the 'minibon' - transferable via the registration in what the legislator defines as a 'shared electronic registration system'[2].

This major evolution in regulatory standing allowed for blockchain to be included in French law for the first time.

Article 120 of the law of 9 December 2016, dubbed 'Sapin II'[3] followed on from this. It gives the French government with the right to take all legislative measures necessary for the adaption of the laws applicable to financial and transferable securities, to allow for the representation and transferral via blockchain technology of financial securities which are neither submitted to the operations of a central depository, nor delivered through a system of financial instrument settlement.

In March 2017 the French Treasury launched public consultation on a draft legislation aiming to adapt French legislation to blockchain technology as part of the above-mentioned Sapin II enabling law[4].

[2] Article L223-12 of the Monetary-Financial Code.
[3] Law n° 2016-1691 of 9 December 2016 relating to transparency, anti-corruption and economic modernisation.
[4] Public inquiry into the project of legislative and regulatory reform relating to blockchain, by the French treasury, 24 March 2017.

OBJECTIVES OF THE REPORT

THE MAIN OBJECTIVE OF THIS REPORT IS TO MAKE AN ASSESSMENT OF ASSET MANAGEMENT AND POST-TRADING/ASSET CUSTODY ACTIVITIES

The Paris financial centre is internationally renowned for its capacities in post-trading activities, i.e. operations following the transaction between a buyer and a seller of securities performed OTC or on regulated financial markets. These operations include confirmation, clearing, settlement, book-entry, asset servicing etc. Three of the ten biggest entities in the world in this domain. Blockchain technology could spark important evolution in these activities. French entities in the field of asset custody have wisely devoted a significant proportion of their R&D to the uses of this technology.

Besides post-trading activities, the Paris financial centre ranks as a global leader for asset management. Nearly 650 asset management companies (AMC) operate in France. Of the global top 20 groups, 4 are French. The French market is also reputed for its considerable entrepreneurial make up - over two thirds of which are AMCs, which boosts its capacity for innovation in terms of maintaining cutting-edge services and business models. AMCs in France manage €3.8tn, €1.8tn of which is managed in French domiciled funds, and €2tn in the form of mandated investments and foreign domiciled funds. Asset management is responsible for over 85,000 jobs, 26,000 of which are in asset management companies. With a 28% market share[5], France is the market leader in continental Europe, well ahead of Germany (15%) - a position which is likely to be reinforced if Paris benefits from the transfer of activities from London, following the UK's departure from the EU. Yet, AMCs have long argued the importance of having a better understanding of the end investor, but also to have better control of the distribution of mutual funds. There too, blockchain can provide interesting solutions, as shown by recent initiatives in Paris and in other European financial centres.

[5] *Asset Management in Europe', 9th edition, May 2017, EFAMA*

Finally, The Paris financial centre is one of Europe's most active in terms of private equity, with €14.7bn raised and €12.4bn of capital invested in 2016. Here too blockchain could provide solutions in terms of account management and simplified transactions of securities held by this industry.

For all of these reasons, the Paris financial centre appears to hold a trump card, when looking at the aspects of competitiveness that blockchain could provide, particularly since it already has a particularly large ecosystem involved in blockchain technology.

EXPANDING REFLECTION BEYOND POST-TRADING TO OTHER FINANCIAL ACTIVITIES

The use of blockchain technology need not reduce itself to the activities mentioned above in the field of finance. Many other branches of finance could be affected by this technology, whether that be in financial markets, funding international trade or insurance. A number of developments, reflections and recommendations may inspire, even apply themselves to these activities, which is why this report proposes to linger briefly to consider some of them.

ANALYSING THE LEGAL FRAMEWORK APPLICABLE TO BLOCKCHAIN

Technology does not require law to innovate and evolve. Financial matters are, however, strictly regulated and controlled on the national and international levels. The application of blockchain technology to the practice of regulated activities, which of course overhauls their uses and practices, therefore requires the definition of legal jurisdictions,

whether that be to propose desired changes to applicable laws, or, on the contrary, to ensure that the law doesn't limit the use of this technology.

PROPOSING THE ADAPTATION OF FRENCH REGULATION

The primary aim of this report is to identify, in the area of post-trading operations, the legislative adaptations necessary for the broadest possible range of uses for this new technology, and in the area of asset management, the issues it raises.

Since the subject is at once technical and unclear, it is vital that financial stake holders work together with legislators. The fact remains that blockchain technology is still far from reaching a point of maturity, and so it is particularly difficult to predict how it will evolve in the future, as much in technical terms as conceptual. Conceiving an elaborate legislative framework therefore risks numerous pitfalls resulting from not having a clear idea of the goals. Consequently, it is necessary to draw the legislator's attention to the importance of taking into account the evolving character of this technology, and to not restrict its growth with overly strict regulations.

France was the first country in the world to legislate for blockchain, to define it and recognise its use. Despite the ruling regarding the authorisation for blockchain to be used for the transfer of 'minibons' going relatively unnoticed in France, it has however caught the eye of the blockchain community.

It is up to the French legislator to keep the ball rolling, and to support the development of FinTech companies in France. Nurturing the ambition to become one of the pioneers of the sector, it is by providing the means to conceive audacious legislation which is devoted to the practice of financial technologies, that France will be able to achieve its objective.

I. PRINCIPLES OF BLOCKCHAIN OPERATION

It is not the intention nor purpose of this discussion to reformulate what a great many reports and books have already elaborated on with regards to the operation of blockchain. The objective here is in part to review the essential operation principles of the technology, but also, and especially, to ponder those aspects which are rarely considered outside the milieu of experts and specialists.

In this regard, it is worth clarifying that blockchains may be considered as pecific forms of distributed ledgers, and that for this reason 'blockchain technology' and 'distributed ledger technology' are often amalgamated. In as far as the notion of a ledger being crucial to post-trading activity, it is easy to understand the interest in blockchain from those deliberating on the architecture of the financial system and possible means for its improvement.

Distributed ledgers allow users of an electronic network to record and manage the data relative to the operation of the network. The information managed by this shared ledger may vary depending on the design of the system, but typically deal with various transactional data: the trading price of securities or physical assets, their virtual identification, etc. This information is distributed among the users who may then use it to settle their trades without the need for a central system of validation.

A distributed ledger such as blockchain requires the following:

- a peer-to-peer network which is either public, partially or totally private;
- a distributed database acting as a ledger, where all transactions and other relevant information is recorded for network members;
- a variety of tools and cryptographic processes ensuring the security of the network - in particular against attacks or attempts to corrupt the distributed ledger - and the integrity of exchanges among its members;
- a consensus algorithm managing the updating of the ledger and allowing for the process of validation of transactions among the members of the network to be automated through a variety of procedural rules;
- an incentive mechanism embedded in the network's operating protocol, which is necessary for rewarding the most active members of the network - that is, those who take responsibility for ensuring that the network works correctly and is secure, especially if the network is completely open.

A. WHAT IS BLOCKCHAIN?

The term 'blockchain', much used in the past couple of years, refers to different concepts, some of which are more precise than others, depending on the context and who uses them. Strictly speaking, the first blockchain was that of Bitcoin using the protocol of the same name. It consists of a database structured as a chain of blocks of information, where the blocks are connected to each other by cryptographic linking for the purposes of making the data stored incorruptible.

This register acts like the accounting ledger for the network, in which all valid transactions are recorded. It is *distributed* in the sense that every active participant of the network - or 'node', has their own copy of it, which they can consult and, if desired, change, by solving a cryptographic puzzle. There is therefore no need for a centralised controller, and the addition of a new block of information to this ledger happens on average every ten minutes, according to a consensus protocol which allows all active members of the network to verify the validity of the proposed transactions.

Since the launch of the Bitcoin network in January 2009, several other P2P (peer-to-peer) electronic networks, with a similarly structured and distributed database - a chain of blocks of information - have come into existence. As such, today we talk about blockchains in the plural form[6], as this term is often used to mean both the network as a whole and its operating protocol. Formally put, a blockchain is a

[6] *For example Nxt (https://nxtplatform.org) or Ethereum (https://ethereum.org), or CoinMarketCap (https://coinmarketcap.com) which lists many alternative ecosystems of blockchain type.*

distributed database which records the transactions of a peer-to-peer network[7]. In everyday parlance, the term implies the entire ecosystem that it encompasses.

However, not all distributed databases necessarily are structured as a chain of blocks, and strictly speaking, blockchains merely are specific cases of distributed ledgers. In the English-speaking world, 'distributed ledger technology' (DLT) is spoken of generically, whereas the order mentioned above relating to minibons refers to a 'shared electronic recording system', which also includes shared ledgers which are not in the form of chains of blocks[8].

B. CENTRALISED MODEL VERSUS DISTRIBUTED MODEL

The first networked IT structures and database management models were centralised, information networks being generally structured around a mainframe, to which passive terminals were connected.

With the development of the internet, the client-server environment with a decentralised network became common - one or several servers responding to their clients' requests - but with a centralised model of centralised data management. If the client-server structure, especially in its more advanced versions, was a step towards decentralisation compared to a structure dependent on a mainframe, it did not completely rid itself of the asymmetry between the server - typically managing the database and its access rights - and its clients.

The first distributed networks then came into being, such as peer-to-peer networks, where each node of the network can simultaneously be both a client and a server, and where there is a potential symmetry between all the nodes on the network[9].

It is important to understand the distinction between the physical architecture of an information network and its organisation model or operating protocol - in particular with regards to data management. It is therefore possible, even on a physically distributed network where all the nodes potentially have the same capacities, to operate a centralised service, for example in the case of a network where there would be only a single server assigned for all clients. Moreover, not all functions of a peer-to-peer network are necessarily perfectly decentralised: Napster, one of the first peer-to-peer networks, initially used a central depository for the exchange of music files between its users, and therefore did not have a functional organisation that was completely distributed.

An essential question for a record commonly held by a community of users is that of reading and writing rights on the database, and more precisely, of knowing who manages these rights and how. Traditionally, the management of a database is centralised with an entity responsible for the distribution of reading and writing rights which therefore controls access to it. Let us suppose that the database fairly reports the different account balances of the clients of a bank. The bank could for example ensure that each client has their own account number and that the same client cannot make two consecutive payments if the sum exceeds the available balance. According to the explicit and implicit contractual agreements between them, the client expects that the bank will ensure that the system and all its operations are well managed and secure. The bank, as centralised body responsible for the management of the financial network's banking data, is acting as depository for their assets just as much as for their trust.

C. TRUST IN A DISTRIBUTED NETWORK

The problem of trust in a record available to an entire network may be easily resolved by designating a trusted centralised body. This body will be the last resort authority for the members of the network should any problems arise. Taking another banking example, if a client claims to have made a transfer to another client, who claims to have not received it, they can both consult their bank, which will settle the dispute. If the centralised body is effectively irreproachable, then the clients can expect a simple resolution to their problem. This entire system would collapse however if the central authority turned out

[7] More precisely, this database is structured as blocks of information, linking one block to the next cryptographically. This cryptographic chaining is important as it allows for any alteration to the data to be easily detected.

[8] Two main texts exist today which make explicit reference to this notion of 'shared electronic recording tool': the order concerning 'minibons' and the law 'Sapin II'

[9] We will not go into detail here about the precise distinction between a decentralised network and a distributed network introduced by Paul Baran of Rand Corporation in the 1960s, the ideas of which led to the first distributed networks in 1969 financed by ARPANET, effectively a precursor to the Internet. We could for example look more into the subject here: https://www.rand.org/about/history/baran.html

to be corrupted, subjective or arbitrary, for example by introducing mechanisms of censorship aimed at certain types of clients.

In the wake of the financial crisis of 2008, and the resulting crisis of trust in institutions, the paradigm of the first blockchain - that of Bitcoin - is precisely to avoid this form of centralised management, and to propose a protocol that does not require any trusted third party[10]. In the pioneering and foundational article by Satoshi Nakamoto, the creator of Bitcoin, the desire to be rid of intermediation of banking institutions is clear and accepted[11].

In a network that is open and accessible to everybody, the rules that govern how the network works must however come and replace the trusted depository. 'Honest' users will only use a public blockchain provided they have the assurance that possible 'dishonest' users will be incapable of undermining the integrity of the network - for example by falsifying transactions etc. The strength of the Bitcoin protocol is precisely that it provides, for the first time, a collection of rules which allow for the trust in an institutional authority to be substituted by trust in a protocol. It is a switch from a standard transactional model to a blockchain model. In order for this to happen, it was necessary to simultaneously resolve the problems which had been identified, such as the 'Byzantine Generals' Problem', and the 'Double-spending Problem'.

D. CONSENSUS AND REMUNERATION

Considering that blockchain is a peer-to-peer distributed network used by thousands, or millions, of users, the question of knowing how this vast community is be able to agree on how this ledger is updated, is natural. It would be possible to go from one extreme to another, that is, from the monopoly of a single centralised body making unilateral decisions about the validity of transactions, to a situation where every transaction is validated by all users.

The dynamic evolution of the network's consensus, that is, the updating of the distributed ledger, must be performed in a methodical and reliable manner. Any change made to the ledger must be consensual (all honest members must agree on the validity of the transactions), reliable (only honest transactions are validated) and efficient (governance must not end up being too costly relative to the objectives).

Although many consensus protocols exist, only the mechanisms of 'proof of work' (PoW) and 'Proof of Stake' (PoS) will be discussed here.

Proof of Work requires from a network node that wants to update the blockchain to show that it has solved a cryptographic puzzle before it can modify the database by adding a block to it. In short, this mechanism ensures that whoever wants to edit the database is required to pay a fee to do so. The sum of all these fees paid will be found in the complexity of the cryptographic calculation of the chaining of the information blocks, and therefore in the security of the distributed ledger.

The Proof of Stake approach is derived from another philosophy: to modify the state of the network, a member has to show that it is already involved in the system. Without a mechanism for adjusting and moderating the different participations at a particular moment, this type of mechanism risks creating a concentration of power by allowing network members that already participate considerably to dramatically strengthen their participation, which risks damaging - even ending - minority participations[12].

Establishing consensus is even more difficult - and costly - as it is necessary to interrogate and coordinate many participants who do not know each other and who do not necessarily trust each other. This is where the fundamental distinction between a public or private blockchain (or semi-private[13]) comes in. The former is open to everyone, without the necessary permission of the other members of the network and allows anyone to become a node. A private blockchain, for its part, functions like a club, where permission is required for entry. This distinction is essential and explains the schism sometimes seen between the supporters of each paradigm of organisation. For supporters of public blockchains, the concept of a private blockchain is nonsensical: having to obtain permission to become

[10] The tide that carried Bitcoin highlighted various advantages of a distributed model compared to a centralised model based on a trusted third party according to different perspectives: political (no potential for abuse of power by the third party linked to its capacity to censure or exclude some participants; economic (increased efficiency with lower costs; security (much more difficult, even impossible to 'attack' a distributed database, etc.

[11] Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto, 31 October 2008: https://bitcoin.org/bitcoin.pdf

[12] A classic problem, also found in the relationship between shareholders and the company's governors

[13] To make it easier, we will not specify here possible nuances and graduations between semi private and private blockchains and we will consider as private any blockchain requiring an authorization to be joined.

a member of the network is an extension of the very institutional censorship that Satoshi Nakamoto wanted to avoid - a centralised model where the monopoly becomes an oligarchy. For supporters of private blockchains, the price of consensus between a multitude of anonymous participants is often considered excessive and useless: they often hold a logic of consortium and are primarily interested in all participants holding a common record; however, the latter are already more or less familiar with each other. It is understandable that, for these people, the temptation is to eventually have a protocol of consensus of proof of participation rather than proof of work: a club has already carried out a selection process of its members, and, in theory at least, these members trust each other - so to revert to a system of anonymous governance where everyone has to be wary of everyone else would effectively be a step backwards.

One could imagine a compromise between the two extremes of a ledger that is completely public and open to everyone and a private ledger only accessible to a few members - a continuum of trust among participants, for whom there is a 'fair price' for establishing consensus and securing the network.

E. CRYPTOGRAPHY AND THE RESILIENCE OF ALGORITHMS

Blockchain security, a vitally important subject, is primarily founded on cryptography of different levels of complexity[14]. The first basic principle is that of the hash function. The defining characteristic of a hash function is that while it is easy to calculate the output y = H(x) for a given value x - the input, it is however virtually impossible for a given y value to find x, such as H(x) = y. Just as opening a safe without knowing the access code would require trying all possible combinations one by one, inverting a hash function, i.e. finding an x that produces a given y, would force the person trying to solve the problem to test a series of entries randomly until they find the solution. Contrary to many codes found in our everyday life which are no longer than a few digits, hash functions are somewhat more complex. For example, for the function SHA-256, the output (y) will be a series of 256 bits, which gives $2^{256} \approx 10^{77}$ possible combinations before finding the correct one - which is nearly as many as current estimations of the number of atoms in the known universe[15]! This last aspect is essential: trying to find any given output from a literally astronomical number of entries results in the virtual impossibility of inverting this type of function with current means of calculation[16].

Hash functions have many uses, such as proving the integrity of a message. It would be sufficient for example, for User 1(U1) to send a message (M) to User 2 (U2) with their digital signature y =H(M). Assuming the signature received by U2 has not been altered, (i.e. y'=y), U2 can verify that the message received from U1 has not been corrupted en route by calculating their digital signature and comparing it to y. Another use of these hash functions in blockchains is precisely to be able to allow blocks of information to be linked one after another and to be able to detect easily any modification made to this chain of blocks. Let us imagine for example a book where, at the bottom of each page N is written its digital signature, TN which is calculated from the text on the page N and from the digital signature of the preceding page. For the first page, we would calculate only $y_1 = H(T_1)$. Any alteration - even just swapping two characters - to an intermediary page I would have a domino effect all the way to the digital signature on the bottom of the last page which would represent a digital signature, calculated recursively, of the entire book. One could therefore immediately look for the alteration of the text on the first page where the digital signature had been modified.

Another essential development in encryption was the appearance of asymmetric cryptography with the work of Diffie and Hellman in 1976[17] and the application of the principles conceived by Rivest, Shamir and Adleman in 1978[18], who are now known worldwide for the asymmetric cryptographic algorithm called 'RSA'. This ground-breaking step[19] allowed, for the first time, two individuals to communicate secretly without having first established between them the encryption/decryption protocol. This contrasts to previous cryptographic techniques known as symmetrical, where the issuer and the receiver had to have already agreed on the manner in which the messages were to be encoded and

[14] *Cryptography is not the antidote however. In the Bitcoin protocol, the fact that the ledger is shared, duplicated and can be consulted by everyone provides an important element of reliability outside of all cryptographic security. The fact that all members are able to view all transactions on the ledger allows for the detection of any attempt to alter it.*
[15] *In the order of 1080.*
[16] *We will not here delve into the considerations of the risks posed by the emergence of quantum computers, (or quantum-proof, already conceived by some protocols.)*
[17] *New Directions in Cryptography, Whitfield Diffie and Martin E. Hellman, 6 November 1976*
[18] *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, R.L. Rivest, A. Shamir, and L. Adleman, February 1978*
[19] *The French cryptologist Jacques Stern writes in La science du secret (The Science of Secrets) (Odile Jacob, 1998) that the progress by Diffie and Hellman is so fundamental for cryptography that we talk about life before and after.*

then decoded[20]. With asymmetric cryptography, U1 can send a message to U2 using a personal key, and U2 in turn will be able to decode the message using the public key known by all U1s. The advantage of this approach is that it allows U1 to be able to use a means of authenticity verification deemed secure by all network members to prove the authenticity of all messages sent: in this way, all messages decoded using one's public key but which had not been encoded would be nonsensical. Inversely, any member of the network, U2 for example, may communicate secretly with U1 by encoding the message sent to U1 by encoding it using U1's public key. U1 is therefore the only one capable of decoding such a message, as, for it to be intelligible, it has to be transformed using their private key that only U1 knows.

The concept of asymmetrical cryptography has paved the way for the emergence of numerous digital signatures. It is vital to understand that the combination of electronic signatures and distributed ledgers allow for any member of a network to transfer the ownership of digital tokens, opening all sorts of possible applications. These tokens can be considered as units of value belonging to the distributed ledger - crypto-currencies and virtual currencies - or as virtual identifiers of other assets - property titles for example. This opens the possibiliy of representing securities and account units to pay for them on the same ledger - that is, of having the securities account and cash account on the same ledger, therefore allowing for an integrated settlement- delivery system.

F. CODE IS LAW

The idea behind the expression '*code is law*', quoted from the American attorney Lawrence Lessig[21], who has since become famous, highlights how, surreptitiously, practices in cyberspace are ruled by the possibilities and limits of computer code, and how these practices may eventually surpass, or even replace, its legal and constitutional predecessors. By defining the forms of our uses of cyberspace and a growing part of our lives, code may become, in one form or another, a legal power - at least for the practices that it imposes implicitly.

Transposed to the context of DLT, the principle is the same. In a blockchain that is open to everyone, the trust that it is possible to have in the integrity of the network stems indeed from the expectation that the rules of operation imposed by the code cannot be broken. From the point of view of an 'honest' user, it is irrelevant whether the other users of the network are honest or not, well-intentioned or searching for a loophole to exploit. If one can trust that the code cannot be corrupted or hijacked, the question of others' intentions is no longer relevant. This is why some refer to blockchains as "trustless systems", i.e. systems where the question of the trustworthiness of the counterparties to a transaction is irrelevant. Trust is shifted from a trusted intermediary depository to a protocol in charge of operating and executing a system of rules in an infallible way. This infallible characteristic of code is not without its risks and may seem unrealistic to those who have written code, as is highlighted in the problem of *The DAO*, which will be discussed in further detail later.

Reversing the question also is interesting: can the law be coded? Can its essence be transcribed into lines of code which could cover all the scenarios and contexts of its application exhaustively? Considering the fallibility of human expectations, the answer clearly seems to be negative. If it is perfectly understandable to hope to implement a system that is as reliable as possible, it would appear that it is also essential to envisage, for all automated transaction platforms, resolution procedures - like those which exist today in different areas of the financial and insurance sectors.

G. DATA TRANSFER SPEEDS ON THE NETWORK

Transfer speeds are an important concern for all networks, whether they be payment or post-trading networks. This vital question has divided the Bitcoin community in the past, both with regards to objectives and means.

One of the triggers for this divergence of opinion lies with the pressing need for an increase in transfer speeds. While for some it was essential for the development of the network that it be capable of dealing with more transactions - in particular in order to have a bandwidth comparable to that for credit cards, others argued that the Bitcoin network was not designed for all payment activities. It was

[20] The code, said to have been that used by the emperor César, consists of changing the characters according to a certain number of steps, decided in advance. One of the simplest examples of which being: by shifting the letters of the alphabet forward one place, 'Hello' becomes 'Ifmmp'.
[21] Code is Law, Lawrence Lessig, Harvard Magazine, January 2016: http://harvardmagazine.com/2000/01/code-is-law-html

therefore asserted that it was as useless to submit micro-transactions directly to the Bitcoin blockchain as to use an extremely secure vault to store loose change. Different paradigms of use were put forward where the Bitcoin network would be used as a depository for digital fingerprints on the day-to-day balance sheet of secondary and peripheral network (sidechain) activity. Another point of contention concerned the technical means necessary to increase transfer speeds, with a lively debate arising within the bitcoin community around the necessity of increasing the maximum size of blocs, which is still today capped at 1 megabyte (1Mb).

These discussions are examples of the challenges of governance encountered by this open community, which can result in certain divergences or 'forks', following the decisions of the most active participants in the network's operation - the 'miners'. A consensus appears to have been reached for the evolution of the protocol Bitcoin Core, dubbed 'segwit', which in August led to the adoption of the proposal *segregated witness*[22] which could have given rise in November[23] to the doubling of the size of a block to 2Mb (segwit2x).

For the financial applications mentioned in this report, and following the envisaged distributed ledger platform, its public or private character and its transaction validation protocol, the technical questions linked to the transfer speeds of the network may change significantly. As such, on the Corda platform proposed by the consortium R3, the validation of transactions is performed directly between the counter-parties via a point-to-point connection, without publishing the transactions to the entire network, and without a mechanism of proof of work or proof of participation. If Corda uses standard blockchain concepts like the use of oracles, ie. external parameters provided by the platform's framework and for whom values cannot, in theory, be contested by participants, then this consortium platform is a long way from the Bitcoin protocol[24].

Generally speaking, the less restrictive the protocol for the validation of new transactions in terms of calculations, the easier it is to increase the speed of processing them. There is a compromise to be found between security and speed and the fact of whether the shared ledger is public or private, is a determining one. Each perspective has its fans and critics.

H. SMART CONTRACTS

Although the Bitcoin network has many more applications than just the simple transfer of Bitcoins, it was initially designed, as stated in Satoshi Nakamoto's article[25] to provide a peer-to-peer electronic cash system. Often stemming from a desire to generalise the functions realised by a blockchain beyond that of simple payment, different ecosystems appeared in the wake of Bitcoin, such as Ethereum, where this desire to generalise was explicit. To draw a picture, in the case of Ethereum, the ledger's data is not only for the purposes of keeping a record of electronic cash but may also be used to execute a programme distributed across the network - called a 'smart contract' - and with which all members of the network can potentially interact.

The term 'smart contract' may be misunderstood if 'smart' is interpreted to mean 'intelligent', then this implies that traditional contracts are 'stupid'. The intelligence that this term, coined by Nick Szabo as early as the 1990s, alludes to is rather that of the facility of management and execution of the terms of the contract - its 'enforceability'. A smart contract's design enables the execution of this programme, i.e. the collection of lines of code, to be as fluid and intelligent as possible. A good smart contract can therefore be defined as a contract that allows for an automated execution and lack of ambiguity of its terms and which thus reduces the risk of disagreement.

By distributing smart contracts on a network, we are moving towards automating as effectively as possible the different management processes of transactions, in particular post-trading activities.

[22] Segwit, which was the subject of the Bitcoin Improvement Proposal (BIP 141), allows, by structuring differently the data specific to transactions and their electronic signature, to retrieve storing space given a constant number of transactions and therefore to process more transactions in average by block and increase the network's flow.
[23] In block 494 784.
[24] For example, Corda also possesses an entity in charge of controlling users' access, called 'Doorman'
[25] Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto, 31 October 2008, https://bitcoin.org/bitcoin.pdf

I. FOCUS: THE BYZANTIN GENERALS' PROBLEM

Anyone interested in the blockchain remembers the first time they heard of the Byzantin generals' problem, which seems to give blockchain a quasi-templar status.

It was the founding study by Leslie Lamport, Robert Shostak and Marshall Pease, published in 1982[26] which borrowed this parable to flesh out their study into logical investigations financed in part by NASA. This study into the verification of the reliability of transmissions using logical reasoning needed a traitor, even several traitors. So, what better environment than Byzance to bring together in the same space and time an extreme organisation - Byzantine - and the elements of darkest duplicity? We could of course question the relevance of this choice of reference and the historical and orientalist prejudices that it may prompt - this is not however the object of this report. Whatever the case, these generals were arguing amongst themselves about how to coordinate either the attack or retreat from the doors of a city that they had surrounded (the city of cities?), without being sure whether the orders they receive would be correct. The dilemma remains to this day. These generals made it possible for the essential mechanism of logical reasoning to be described in layman's terms. Lamport, Shostak and Pease's work was based on this concept of verification of information transmitted within an organisation.

Obviously, the article was not concerned with blockchain at the time of writing, but rather with the general transmission of information via computers. As the writers explain:

'A reliable computer system must be able to cope with the failure of one or more of its components. A failed component may exhibit a type of behaviour that is often overlooked--namely, sending conflicting information to different parts of the system... We devote the major part of the paper to a discussion of this abstract problem and conclude by indicating how our solutions can be used in implementing a reliable computer system.'

The next part of the study considers different hypotheses, each concluding with a logical rule. The first rule dictates that, in the case of simple oral transmission, only situations in which the traitors represent less than a third of the generals may be identified. Otherwise, the orders transmitted by the disloyal general(s) would be mixed up with the true orders and would confuse the loyal generals, resulting in their actions being uncoordinated.

The rest of the study gradually approaches more and more complex situations before finally reaching the conclusion that in the case of written messages rendered unfalsifiable, the logic problem may be resolved by the loyal generals, regardless of the number of traitors in their midst. By 'unfalsifiable message', the authors mean neither a true message - since the message could have been written by a traitor or by a loyal general under duress from a traitor - nor an encoded message.

One of the important take-aways of this study is that, in a chain of orders, by matching the message of an algorithm which performs side calculations, for example during a period of time which cannot be reduced before the message is forwarded to the next recipient, the recipient will know for sure if the message is part of a reliable chain of messages or if part of the chain had been interrupted or falsified, and consequently would be able to adapt his reasoning and verifications.

The influence and relevance of this analysis for the research which followed it is clear. Blockchain owes a lot to this analysis which connects the transmission of information in a network, with the verification algorithm used by the network's operators, and is arguably directly descended from it. This article's publication added a new impetus to the first studies of the 1980s by refocusing the attention on the chain itself as not only a means of more or less reliable transmission, but as a means of storing and proving.

The solutions produced from the problem of the Byzantin generals also highlights a principle which is also an ontological limit to the functioning of the blockchain: effectively, the chain must be perpetually verified by the members of the network if its validity is to be maintained. As the writers conclude later, the solutions that they propose are necessarily costly, as they 'take time and use a lot of messages.' This is one of the challenges that the blockchain today must overcome.

[26] *The Byzantine Generals Problem, Leslie Lamport, Robert Shostak & Marshall Pease, 5 July 1982*

II. THE USE OF BLOCKCHAIN IN FINANCIAL MARKETS

DLT seems to hold great potential for financial activities, in particular financial markets. The main reasons being the decrease in the cost of transactions, due to the reduction in the number of intermediaries. According to a study by Oliver Wyman quoted by professor Michael Mainelli[27], the annual cost worldwide of the processes of clearing and settling in the financial markets is estimated to be over $40billion, essentially because of the need to settle transactions. Other overhead costs include ensuring the security of transactions, and increasingly fast conclusion of the transactions' life cycles.

A. PRIMARY MARKET ACTIVITIES

Beyond using the technology as an operating procedure for an exchange system, the blockchain has also found, through cryptocurrencies, a use as a way of raising capital, in place of traditional stock and equity markets.

For several months already, a new form of public offering has been flourishing[28], not only because they deal with start-ups, but mainly because they are in the form of cryptocurrencies, like Bitcoin (BTC) or Ether (ETH), from whence comes the initialism ICO - Initial Coin Offering, with reference to IPO - Initial Public Offering. These operations are a quick way of securing financing - capital can be raised in as little as a few hours to a few days - for entrepreneurs in the world of DLT, allowing them to test their ideas or project on a community of experts. Taking into account the potential of this technology, these capital raises also attract more and more investors looking for added value, even if they do not always understand the technological specificities of the project.

An ICO is relatively informal - the capital raise is carried out within the framework of a whitepaper, which details the founders, the project, the need for financing, the future allocation of capital, the ICO process and the cryptocurrency payment conditions. These capital raises are made online on special websites. In most cases, the organisation promotes its project by presenting the team which is developing the 'token' which is issued following the ICO, its source code, the conditions of issuance etc. The sums raised by the ICO are generally in the form of BTC or ETH. The interested 'investors' then receive tokens in exchange for their payment. These tokens represent a sort of 'economic interest' in the company: depending on the project, they can have different uses, and eventually allow the holders to receive the fruits from the development of the project, especially if the raise is for the purposes of financing the R&D and test phases. They never have access to the capital of the company. Once the raise is complete, it's possible to trade the token on the secondary market on special platforms.

Among the main differences between ICOs and traditional capital raises can be noted:

- Minimal identification of parties: investors often do not need to identify themselves on the platform. Similarly, issuers perform little or no ID verification on the investors or their sources of financing;
- The amount raised is transparent but may be manipulated: BTC and ETH payments are recorded on public chains of blocks, allowing anyone to see the quantity and amounts that go towards the ICOs address. However, while the amounts invested are transparent, it is difficult to know who sent them. This means that it is nearly impossible to know if the project is the subject of real success or if the raise is artificial as a result of the presence of the issuer itself in the raise;
- Premium for first investors: often, crowdsales are offered in levels whereby earlier investors are offered a better price than later investors;
- Retention and price discovery: usually, the project does not submit all of the tokens to the

[27] *The impact and potential of blockchain on securities transaction lifecycle, M. Mainelli and A. Milne, 9 May 2016, http://www.swiftinstitute.org/wp-content/uploads/2016/05/The-Impact-and-Potential-of-Blockchain-on-the-Securities-Transaction-Lifecycle_Mainelli-and-Milne-FINAL.pdf*

[28] *One of the first documented uses of an ICO for a cryptocurrency project was Mastercoin, completed by the forum Bitcointalk. Mastercoin is a meta-protocol on the Bitcoin blockchain which provides the supplementary functionalities that the basic level of Bitcoin does not have. The ICO happened in 2013: Mastercoin (MSC) raised over 5000 Bitcoin (BTC) at a rate of 100 MSC: 1 BTC.*

offering, but instead keeps a certain number of them, particularly for the management - for example, 60% of tokens are sold in the ICO, and the projects keeps 40%;
- Ceiling and floor: sometimes minimum and maximum limits are added to raises. If the minimum is not reached, the investors are reimbursed, and the project is abandoned. Once the maximum is reached, no more tokens are distributed.

ICOs incorporate notions from both donation and investment.

Attempt at defining the term token

There are various different types of token, each with different characteristics and uses. Some tokens, like BTC, work like a cryptocurrency, while others can represent a right to tangible or intangible goods. The tokens in a blockchain can also be used in new protocols and networks to create distributed applications. As a general rule, issued tokens can confer the rights to future profits earned by the start-up and/or voting rights in the financed project. These tokens, sometimes called application coins - or 'AppCoins' or 'Protocol Tokens', represent the next phase in innovation in DLT and the potential of new types of decentralised models: for example, cloud computing without Amazon, social networks without Facebook or online marketplaces without eBay.

The biggest cryptocurrency players of the world banded together to create the *Blockchain Token Securities Law Framework*[29] as a form of self-regulation. The partnership includes companies like Coinbase, ConsenSys, Union Square Ventures and Coin Center.

Framework for Public Offerings and ICOs

These new ways of financing lead us to ask ourselves questions about their regulation. Several legal regimes are possible in theory (franchise contract, computing license), but it is particularly the analogy of the offering of securities that draws the most questions. Certain tokens, according to their characteristics, can therefore constitute an offense according to federal or state laws on securities in the US. This means, amongst others, that it would be illegal to offer them for sale to residents in the US if they were not either registered with the Securities and Exchange Commission **(SEC)**, according to the Securities Act of 1933, or legitimately exempt from registration. This is the position recently expressed by the SEC, which published a memo insisting that tokens could, according to their characteristics, be considered to be financial securities[30] before considering that the offer of tokens realised by The DAO constituted a public offering of financial securities as per the Securities Act[31], notably because the tokens in question gave access to the potential profits of the issuer. On this occasion, the SEC was able to clarify that the qualification of tokens would be examined on a case by case basis and would depend on the economic reality of the transaction and therefore on the characteristics of the tokens. Although followed a couple of weeks later by Singapore[32], this approach today still does not provide solutions and considerable uncertainties remain concerning the future legal regime of ICOs and tokens.

In as much as ICOs can resemble capital raises, the regulation applicable in the European Union is the Directive on public securities offering, the **Prospectus Directive**[33]. If the conditions listed in the Prospective Directive are fulfilled, then the issuer has to write and publish a prospectus. Among the criteria that define the scope of the Directive, the most important for our purposes is the one relative to the presence of 'transferable securities', the term having been replaced by 'financial securities' when transposed into French law. To what extent do tokens issued by a blockchain qualify as such? This is the crux of the issue and of the debate. While in the US, the Howey test, used to determine whether a financial instrument ought to be considered as a 'security', focuses in particular on the notion of currency, it is rather that of financial securities, or securities, which is at the centre of discussions in the EU. In blockchains such as that of BTC or ETH, tokens represent a value, which does not mean much. These tokens may just as well assume the functions of a value of exchange, as a non-financial asset, or even a financial asset, according to how they are used. It is therefore a case-by-case assessment which is required.

[29] *Major Players Unite to Define Blockchain Token Securities Law,Dom Galeon et Patrick Caughill, 7 December 2016,: https://futurism.com/major-players-unite-to-define-blockchain-token-securities-law*
[30] *"Depending on the facts and circumstances of each individual ICO, the virtual coins or tokens that are offered or sold may be securities". Investor Bulletin: Initial Coin Offerings, SEC, 25 July 2017*
[31] *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, SEC, 25 July 2017*
[32] *http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx*
[33] *Directive 2003/71/CE of the European Parliament and of the Council of 4 November 2003. The Prospectus Directive is to be replaced by Directive (UE) 2017/1129 of 14 June 2017 to be implemented 21 July 2019.*

If these tokens do not fit into the definition of financial securities, ICOs are therefore not subject to the regulation relative to public offerings of securities. Do ICOs therefore escape all regulation? Regulators have yet to clarify their position on this question, including those in the EU. In France, the *Autorité des Marchés Financiers* - Financial Markets Authority **(AMF)** holds sway over 'atypical property' or 'alternative property', which includes life annuity, precious stones, vehicles, diamonds, manuscripts, wine, solar panels etc. When it is subject, as part of promotional communication or door-to-door sales, to the laws concerning chattels and real estate (miscellaneous goods 1) or the acquisition of ownership rights of one or several assets with the express purpose of direct or indirect financial return, or with similar economic effect (miscellaneous goods 2), the AMF is the authority in charge of examining the documentation proposed to the public[34].

Other countries have declared their position on the legality of ICOs or have alerted the public on the risks of these operations:

- The UK financial regulator, the Financial Conduct Authority **(FCA)** in a publication dated 12 September 2017 warned potential investors on the risks associated with ICOs. The publication estimates ICOs to be very risky speculative investments and calls on investors to be very wary of them. The FCA also states that only certain ICOs would probably be within their jurisdiction.
- The Canadian financial regulator, the Canadian Securities Administrators **(CSA)** published a memo dated 24 August 2017 in which it states that ICOs may be subject to laws governing Canadian financial securities but goes on to state that tokens do not necessarily qualify as 'securities' according to Canadian law. The regulator affirms that tokens could also be subject to laws concerning derivative products, if they can be defined as such.
- The Israeli financial regulator, the *Israel Securities Authority* **(ISA)** announced on 30 August 2017 that it would organise a committee to deliberate on the application of financial securities law to ICOs.
- A committee of regulators coordinated by the People's Bank of China published a declaration on 4 September 2017 forbidding all future ICOs and forcing all issuers to reimburse all tokens already issued.[35]
- The financial regulator of Singapore, the Monetary Authority of Singapore **(MAS)** published a declaration on 1 August 2017 in which it states that certain tokens may qualify as 'securities' according to the Securities and Futures Act in Singapore, in which case issuers have to submit a prospectus to the MAS before issuing tokens, except in cases where they are exempt. Moreover, issuers of tokens qualifying as 'securities', or their intermediaries, have to obtain the relevant authorisations as required by the Securities and Futures Act.
- The regulator of Hong Kong, the Securities and Futures Commission **(SFC)** stated on 5 September 2017 that tokens could, according to the individual circumstances of the ICO, qualify as 'securities' with respect to the Securities and Futures Ordinance, which would subsequently require various authorisations and registrations from the SFC.
- The South Korean regulator, the Financial Services Commission **(FSC)** announced on 3 September 2017 that a group had been assembled with other regulators to deliberate on the subject of cryptocurrencies and the regulatory framework. The FSC underlined in particular its desire to tighten the requirements for client identification and the fight against terrorist financing. On 29 September, it eventually forbade any capital raise in the form of cryptocurrency, justifying this measure by the need for investor protection in the face of increasing fraudulent ICOs.
- In a press release dated 29 September 2017, the Swiss financial regulator, the Financial Market Supervisory Authority **(FINMA)** announced the launch of an enquiry into several ICOs. In its 04/2017 Guide, published in April 2017, FINMA states that ICOs may be, depending on their structuring, within the jurisdiction of (i) regulation against money laundering and terrorist financing, (ii) banking regulation relating to the acceptance of public deposits, (iii) the rules applicable to financial securities and derivatives, and finally, (iv) those applicable to collective investment vehicles. As FINMA states:

  "due to the close proximity in some areas of ICOs and token-generating events with transactions in conventional financial markets, the likelihood arises that the scope of application of at least one of the financial market laws may encompass certain types of ICO model".
- The Central Bank of the Russian Federation, in addition to its alerts concerning the risky character of ICOs, announced its desire to restrict ICOs to authorised investors, via Moscow's stock market, before the end of the year[36].

[34] *Article L. 550-1 of the Monetary and Financial Code*
[35] *http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html*
[36] *https://www.cbr.ru/press/PR/?file=04092017_183512if2017-09-04T18_31_05.htm*

B. SECONDARY MARKET ACTIVITIES AND TRADING

The DLT has not only prompted innovation on the primary market, with the appearance of ICOs: it may also have a revolutionary effect on secondary market and trading activities.

Regarding the negotiation phase, the distinctive aspect of this process largely relies on the manner in which an efficient process of order matching and price formation is conceived. Essentially, the ability to use the blockchain, with an added value, for negotiating activities, depends on two factors: (i) the nature of the financial instruments traded, and (ii) the nature of the intended negotiating activity.

Pricing methodology is intrinsically dependent on the nature of the financial instrument in question. For some instruments, the price is merely established through the matching of purchase and sale interests. This is typically the case for equity securities. The pricing of these products therefore requires perpetually centralised supply and demand. This centralisation may be 'real', meaning that all supply and demand of the instrument in question is held on a single platform. It may also be 'virtual', which is the norm for most markets where the sale and purchase interests of an instrument are distributed over several platforms simultaneously. In this latter case, the agreement on price is ensured by arbitrageurs who, in the shortest time possible, ensure a constant link among these platforms. These instruments therefore require not only a certain degree of centralisation of interests but also (as a consequence) the capacity to absorb and deal with considerable volumes in a short space of time.

For these instruments then, the blockchain, as it is decentralised and limited in terms of processing abilities, cannot be used to store an order book without (i) putting pricing at risk and (ii) retreating several decades in terms of order processing capabilities and times, even without considering the blockchain's intrinsic incapacity to contribute to pricing based on the relationship between supply and demand. It is in this respect interesting to note that the order books of cryptocurrency exchanges are currently operated outside any blockchain.[37]

This being said, once orders are matched in an order book, and therefore the question of centralisation is no longer relevant and that of the settlement period less important, the resulting transaction may be created on the blockchain, even before its clearing and settlement. This is even the indispensable condition of the use of blockchain for the purposes of optimising post-trading processes which will be discussed later. With regards to performance (that is, the combination of the size and the coding algorithms), this possibility seems today to be open to a limited number of instruments, those of limited liquidity. It is highly probable that this possibility extends to more liquid instruments as the performance of the blockchain increases.

As an example, concentrating on the question of capability, and disregarding the subjects of centralisation and clearing period, Opimas[38] estimates that the blockchain should reach 1.5 terabytes (Tb) to host all the securities transactions carried out on order books on European platforms in 2015 (without even taking into account the number of upstream orders), a capacity which should grow at the rate of the increase in volume of the relevant markets. Today, the size of the Bitcoin blockchain is around 130,000 megabytes. This increase in size is feasible; nevertheless, it would require a considerable increase in computational capabilities, bandwidth and data storage at the level of nodes and miners, therefore requiring in turn a certain form of concentration, and only a handful of institutions have the means to achieve such capacities. An alternative would be to improve the performance of the blockchain itself by outsourcing part of the verifications to assigned entities outside the blockchain. In that case, the blockchain can only be private, controlled by identified entities, which would again result in a certain degree of concentration.

However, using the blockchain for trading activities is conceivable even before the creation of the transaction for other instruments. This is typically the case for instruments whose trading price is purely bilateral (in particular for exotic derivative products).

The possibility of using a blockchain for trading purposes thus depends on multiple factors. Nevertheless, it can be expected that the application of the advantages provided by this technology to other segments of the value chain will have a major effect on trading activities. In particular, by streamlining the post-trading phase, blockchain is bound to have as much of an impact on the demand as on the supply of capital, by prompting a growing number of capital issuances on the markets and by increasing investment in and exchanges of instruments in circulation and therefore the volumes traded.

[37] *Bank of America Merrill Lynch, Exchange Views – How will blockchain change European market structure, 01 Feb 2016; SWIFT Institute, Working Paper n°2015-007, The impact and potential of blockchain on the securities transaction lifecycle, 09 May 2016; UBS, Global Exchange – The potential impact of blockchain / DLTs on the global equity exchanges*

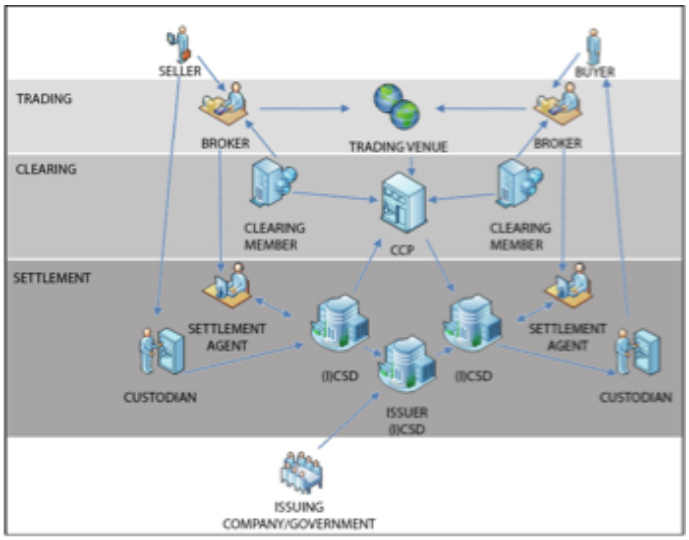
[38] *Opimas, Blockchain for capital markets - A pipe dream, May 2016*

C. POST-TRADING ACTIVITIES

DLT can also simplify the landscape of traditional organisation and operation of post-trading activities.

In the traditional scheme of things, a transaction's life cycle on the stock market requires the presence of a market intermediary, a trading platform and various post-trading infrastructures and intermediaries, including a clearing house, a settlement agent, a depository and a central depository. All these actors play a specific and important role, dating back to the creation of modern stock exchanges in the 19th century. Since then, some links of this value chain were radically transformed, as much in terms of technology (transforming for example, from a physical trading floor to an electronic automated order execution system) as in terms of competition (today, at any given moment, it is possible to process the same security on several trading platforms in Europe). Similarly, stockbrokers have been replaced by banks, national stock exchanges have regrouped into regional collectives, and clearing houses and central depositories have evolved too. The latter, now referred to as Financial Market Infrastructures (FMI), have evolved further from a cooperative share ownership to a capitalist joint-stock share ownership - a change that was referred to in the 1990s as 'demutualisation' or 'privatisation'.

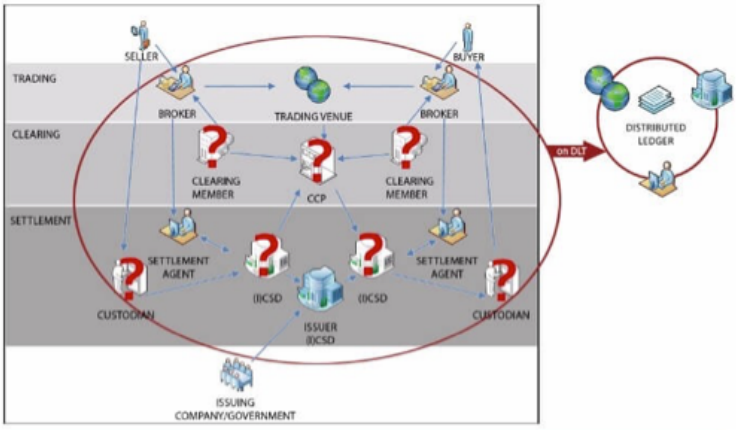
In this model, the instruction to buy or sell a financial security on a stock market follows a complex cycle, both in technical and legal terms, due to the presence of these various entities. It is even sometimes difficult to track an order all the way from the investor to the delivery or payment: the clearing house makes it impossible to track an individual instruction due to multilateral settlement methods.



Moreover, for several years the demands of equity for FMIs as well as for financial intermediaries grew significantly in order to quarantine the risk of default of one party, limiting the effect that it would have on the rest of the trading cycle process.

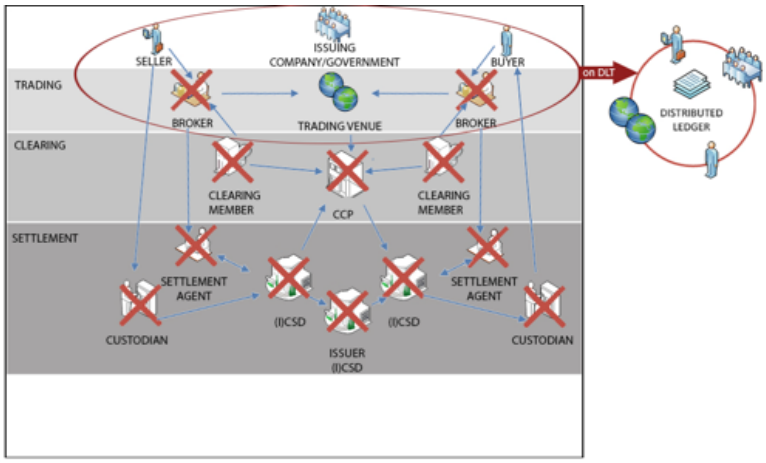
In financial markets, the steady disappearance of paper securities and their replacement with virtual assets has led to the replacement of physical settlement using cash, with digital trades. This is the case too with paper money being replaced by virtual money. The need remains however, for a 'golden record', a way for market infrastructures and intermediaries to keep their individual databases updated by communicating with the other institutions involved at other levels of post-trading, in order to be able to reflect each transaction in the records for each intermediary/infrastructure. The high cost of this type of process provides the impetus for an examination of the possibilities offered by distributed ledgers as an alternative to current centralised systems.

Effectively, a DLT structure could loosen these restraints, and in particular drastically reduce the costs for investors, but also the needs for equity of market intermediaries. Very few studies have been carried out on these equity savings, which would not be identical for all classes of securities, subject to different regulatory rules. But, as the ECB highlights, "DLTs have the potential to address many of the shortcomings identified in the post-trading market"[39]. How? By simplifying the trading process and by rethinking the role of some market infrastructures. Effectively, DLT could assume the role of stock exchange, clearing house and central depository, even finalizing settlement, with all transactions recorded in a decentralized ledger. The question of payment in a public blockchain system is however a delicate one, when considering the use of a cryptocurrency.



[39] *ECB, Distributed Ledger Technologies in securities post trading, revolution or evolution, Occasional paper series, n° 172, April 2016.*

Besides market infrastructures, it is the brokers and intermediaries who may see their role profoundly affected by DLT. As such, there would be no technological reason for stopping each investor having direct access to the DLT for the purposes of negotiating an order, even if such a facility does not yet exist on the market.



All these reasonings work in favour of considering the operational, technical and legal dimensions of using DLT as a substitute for current modes of operation of post-trading activities.

Certain market infrastructures have started work on the benefits that this technology could provide. As such, according to Euroclear[40], the application of DLT in securities settlement could provide the following advantages:

- reduction of settlement periods
- reduction in holding risk
- increased transparency for issuers, end investors and regulators
- reduction of the intermediation in bookkeeping
- increased data security

The major difficulty in this area is a limited experience and a limited number of practical assessments on the impacts of DLT on post-trading activities[41]. The most recent and thorough study certainly is that performed by the Tokyo stock exchange in 2016, which tested the use of DLT for its clearing and settlement activities . In its report, the Japanese stock exchange recreates the lifecycle of a transaction and examines how DLT could alter current procedures.

Clearing and Settlement

Contrary to the trading process, it is not necessary here, even if it is desirable, to aggregate orders in the sense that the decentralised process of DLT could provide advantages such as its rate of availability. It is in this aspect of clearing that the Tokyo stock exchange estimates the greatest impacts. Indeed, as transactions are recorded one after the other, it is no longer useful to use a clearing mechanism: the same transactions are traded, then settled and delivered. The system thus operates in gross – no longer in net – with no need for clearing. Thus, DLT questions the very existence of clearing houses.

Financial securities ownership

The identification of the owners of securities is immediate and above all, complete. Of course, the confidentiality of some information should be ensured, but the principle of the traceability of ownership of each security is a major step forward.

Financial securities transactions

A list of shareholders at a particular date may be obtained retroactively and it is possible to implement financial securities transactions such as dividend payments or assigning rights to certain categories of shares using the list of shareholders.

For all these reasons, the study carried out by the Tokyo stock exchange considers the application of DLT to the post-trading market could make it more efficient in the future. However, the study identified several concerns that could obstruct the short- and long-term deployment of DLT. In particular, the question of synchronisation of clocks between nodes, which may prevent performing transactions simultaneously. Another difficulty lies in the speed of transactions: the transfer speed of DLT, which determines if many transactions can be processed per unit of time, is generally affected by the way the consensus algorithm operates. As mentioned above, increasing transfer speeds requires that the maximum number of transactions by block also be increased, or that a faster consensus algorithm be adopted. The first could be achieved by increasing the size of the blocks; however, this would result in a larger network bandwidth during the consensus process. In fact, everything depends on the type of technology used by DLT.

[40] Euroclear & Slaughter and May
[41] Atsushi Santo & al. "Applicability of the Distributed Ledger Technology to Capital Market Infrastructure", Japan Exchange Group, Working Paper, 30 August 2016, vol. 15

Even if it is too early to draw any definitive conclusions, these different studies highlight the potential of distributed ledger technology. Additionally, innovation is generally welcomed in the European equity post-trading market, where it can reinforce security and efficiency. A certain number of factors may however pose potential problems in the blanket adoption of DLT.

There are several issues to be cleared up before DLT replaces current IT tools in post-trading activities. Whether they are questions of legality, operations or governance, they all need to be examined logically. All this is going to take time: for the ECB, the post-trading revolution is unlikely to happen in the short term, and the process of use of DLT will doubtless be a gradual one and will be a steady transition in parallel with existing tools.

Central Depository

Regulation (UE) 909/2014 of the European Parliament and of the Council of 23 July 2014 concerns the improvement of the regulation of securities in the European Union and the Central Securities Depository Regulation **(CSDR)** states in article 3 that:

> 1. *Without prejudice to paragraph 2, any issuer established in the Union that issues or has issued transferable securities which are admitted to trading or traded on trading venues, shall arrange for such securities to be represented in book-entry form as immobilisation or subsequent to a direct issuance in dematerialised form.*
>
> 2. *Where a transaction in transferable securities takes place on a trading venue the relevant securities shall be recorded in book-entry form in a CSD on or before the intended settlement date, unless they have already been so recorded.*

'Trading venue' in the context of CSDR refers to a regulated market, a multilateral system of trading or an organised trading system. As such, article 3 of CSDR requires issuers whose securities are listed to issue these securities with a central securities depository.

Insofar as the CSDR is directly applicable, the use of DLT for post-trading activities book-entry of listed securities therefore requires the DLT operator, under current regulation, to obtain a license from the **CSD**.

D. ASSET MANAGEMENT ACTIVITIES

1. The implications of blockchain for asset management

Blockchain is a technology that could potentially drive innovation for the asset management industry, both in terms of operational effectiveness and cost reduction and exploitation of information. These various uses may be understood both at the level of asset management – i.e. the investments made by undertakings for collective investment **(UCI)** – and liability management – i.e. the UCI unitholders. Its impact will essentially cover, on the one hand, the flow of information with the stakeholders – depositories, account keepers, asset servicers, distributors, data providers, issuers, etc., and, on the other hand, internally between the various departments. In addition, combined with the possibilities offered by Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market **(PSD2)**, asset management companies may develop activities for direct marketing of UCI to investors.

Assets (non-exhaustive list):	Liabilities (non-exhaustive list):
Post-trading: ongoing project on French small-cap transactions	Settlement and delivery of an investment fund
Voting process at meetings	Direct sale of funds to the investor thanks to PSD2
Management of Securities Transactions	The life cycle of funds including the management of UCI events from creation to dissolution
Collateral management	Monitoring and payment of trailer fees
Share register	Unitholder information, standardised updating of documents (Fact sheet, Key Investor Information Document)
MIF, EMIR, SFTR transaction reporting	Customer knowledge: KYC
AIFM regulator reporting	Order marking

Several projects are in progress with an implementation scheduled for the end of 2017 or the beginning of 2018. It is therefore too early to quantify the returns on investment or to identify any difficulties upon their large-scale deployment. "Blockchainisation" in third-party asset management

can be seen as concentric circles moving further and further away from the asset management company, which is a group subsidiary:

- "In-house" UCI self-consumption, improvement in the sharing and traceability of information within various departments of the same entity: management of reporting, contracts, consolidation of tools and data, etc.;
- Intra-group distribution and dissemination of information (KYC);
- Distribution outside the group but in the same country of its business address; and
- International distribution.

In concrete terms, and beyond the "purely" technological aspect, one of the decisive uses of blockchain for the asset management industry is the management of fund liabilities via the reduction in the number of intermediaries and the improvement in and recovery of customer knowledge.

After introducing the value chain of asset management companies **(AMC)** and their ecosystem, our analysis will focus on the impact of this new technology in the systems for settlement and delivery of UCI units, according to the Clearing and Settlement Depository **(CSD)** and Transfer Agent **(TA)** models.

2. The value chain of asset management companies

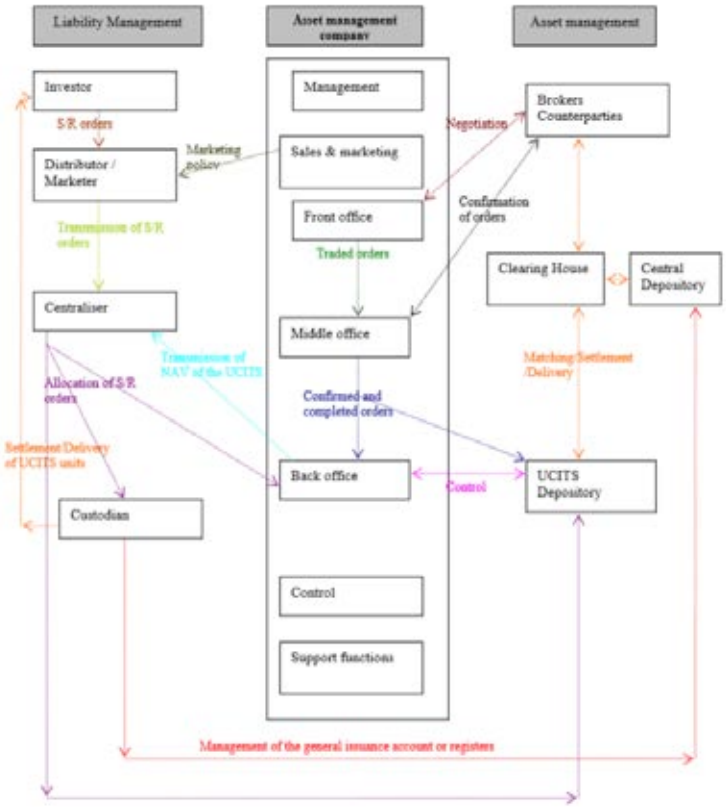
Asset management companies are institutions responsible for financial, administrative and accounting management of products managed on behalf of third parties: UCI and discretionary mandates. Approved for that purpose by the AMF, they undertake to manage independently and in the sole interest of the investor the sums entrusted to them, the managed assets still deposited with the depository/account keeper.

Currently, there is no single organisational framework for asset management companies but rather a multitude of organisational frameworks or asset management models, which the companies adapt according to various parameters such as their specialisation, their investment expertise, their size, the structure of their body of shareholders, their commercial strategy, their partnerships, their distribution methods, etc.

3. The ecosystem of asset management companies

The most recent ecosystem of an asset management company is made up of depositories, custodians, account keepers, statutory auditors, auditors, brokers and centralisers placed in the majority of cases with the account keeper or the depository of the fund.

The Asset Management Company in its ecosystem



There are two key aspects in the activity of the asset management company:

- Asset management which covers all activities related to financial management and constitutes the core business of asset management companies. The main activities are market activities related to allocation, the selection of securities and the realisation of investments: purchase and sale of securities held in the portfolio, placing of orders, trading, confirmation and checking of these orders, etc.; and
- Liability management which covers activities related to the centralisation of unitholders' subscription or redemption orders, settlement and delivery transactions, and for collective management of UCI issuance accounts with the update of the number of UCI units in circulation.

- Liability management therefore involves the distribution process upstream and the management of accounts/the register of unitholders and custody downstream[42]. It may be used by all the AMC's functions: sales, marketing, risk control, financial functions, management, general management. It is both an increasingly controlled regulatory obligation and a key element in the customer relationship and in customer knowledge.

Liability management: tool for customer knowledge

The various stakeholders involved in liability management are:

The Centraliser: receives all the subscription and redemption orders for the UCI units from distributors and checks their compliance with the conditions set out in the prospectus or in the marketing agreement. Once the net asset value is known, the centraliser is responsible for converting the orders denominated in units into an amount, and vice versa. It sends the various information collected to the asset management company, to the issuance account keeper (creation or cancellation of units) and to the UCI depository (movements of funds).

The depository/Custodian: asset management companies can hold neither securities nor cash originating from their customers. The financial instruments constituting the portfolio of their investment vehicles (UCI and physical securities mandates) are therefore, owing to regulation, entrusted to a separate entity, the depository for the UCI and the custody account keeper **(CAK)** for the mandates. The depository's main duties are:

- The safekeeping of the assets of funds or mandates. This involves keeping the securities and cash accounts up to date, holding the titles of ownership of financial instruments, receiving settlement and delivery orders and executing them in cooperation with the central depository or the local or foreign depositories, and finally informing the fund and processing the securities transactions for the portfolios;
- Checking the regularity of the decisions made on behalf of the investment vehicle. This involves verifying the conformity of the investment decisions made by the UCI with laws and regulations and the prospectus (rules on the composition of the assets, risk spreading, etc.). The depository is also responsible for periodically calculating the net asset value, checks the documents produced by the AMC (annual reports, accounts, periodic statements, etc.) and must be able to assess the IT procedures and systems used by the asset management company;
- Monitoring cash flows. The depository must ensure effective monitoring of the UCI's cash flows, be it an Undertaking for Collective Investment in Transferable Securities **(UCITS)** or an Alternative Investment Fund **(AIF)**, with the aim of preventing fraud in addition to combating money laundering and preventing terrorism.

The central depository offers services such as the registration of securities when they are issued, their centralised custody and their delivery for cash in the event of a transaction on the financial markets. In France, the central depository is Euroclear.

The Transfer Agent: In connection with the marketing abroad of their UCITS, asset management companies use a transfer agent, which is an essential intermediary for cross-border distribution. Besides its role as a collector of subscription and redemption orders across the whole country in which they are marketed, it also keeps the positions of each marketer, calculates the expected distribution fees and disseminates the associated reporting information. The transfer agent is therefore in other countries what the issuance account keeper, registrar and centraliser are in France.

Liability monitoring covers:

- Two functions regulated and defined by the General Regulation of the AMF:
  - The function of centraliser may be carried out by the UCI itself, the asset management company, an Investment Service Provider (ISP) or, most commonly, by the depository;
  - The function of issuance account keeper. This function is performed by the UCI itself, under its responsibility: it can only delegate this activity to an ISP and only under the conditions set out in the General Regulation of the AMF. It nevertheless retains full responsibility vis-à-vis investors.
- A practice initially developed to monitor the outstanding liabilities out of which the asset management company undertakes to remunerate a distributor: position keeping for subscribers.

[42] *Gestion du passif des OPC et enjeux réglementaires (UCI liability management and regulatory implications), Kramer Levin, July 2014*

Liability monitoring usually makes it possible to identify the subscribers – institutional investors in the broad sense – and the establishments responsible for keeping retail subscribers' accounts. It identifies the customer or type of customer of the funds. Liability monitoring is therefore an important lever for the commercial development and improvement in the profitability of asset management companies.

A liability monitoring tool is the link between the finance, risk, marketing and sales functions. It represents the necessary basis for any implementation of processes intended to improve and monitor the effectiveness and commercial profitability of the asset management company:

- Customer knowledge and therefore better commercial effectiveness;
- Liquidity of funds risk management, which becomes a regulatory obligation, especially for leverage funds;
- Prospects for management efficiency by adapting asset management to fair liability constraints, paving the way for an asset/liability management for funds.

4. The CSD and Transfer Agent models

According to the Transfer Agent model, orders relating to the funds and the settlement and delivery system are processed bilaterally between the institutional investors or the distributors and the transfer agents. This model is widespread in Luxembourg, Ireland, the United Kingdom and Spain. On the contrary, under the CSD model, adopted in France, Germany, Norway, Austria and Portugal, the infrastructure relating to orders for funds and to settlement and delivery is provided primarily by the central depositories.

This will involve analysing the potential effects of DLT on these two systems, without making any value judgment on the merit of both these systems or establishing a hierarchy between them.

As a preliminary issue, it must be stressed that the development of distributed ledgers is understandably likely to prompt issuers to replace the bearer securities system, which is very popular in France to this day, with the registered securities system which is inherently more compatible with the DLT.

4.1. The CSD model

In France, fund administration is responsible for accounting and valuing UCI assets but not for collecting subscriptions and redemptions of UCI units or for managing liabilities. A centraliser, which is independent from the fund administrator, collects the subscription and redemption orders for the UCI units and, therefore, the latter's flows in liabilities. Its role is limited to flow management: it does not replenish stocks, i.e. liability position keeping.

Pursuant to the General Regulation of the AMF[43], the key tasks relating to the centralisation of orders for UCI units are as follows:

- Providing centralised reception and registration of orders;
- Supervising compliance with the cut-off for centralising orders referred to in the prospectus;
- Reporting the outcome of centralised reception of orders for the UCI as an amount and, where applicable, as the aggregate number of units/shares subscribed or redeemed;
- Valuing the orders after receiving information about the net asset value per unit/share from the UCI;
- Reporting the information that the issuance account keeper needs to create or cancel units/shares; and
- Reporting information about the outcome of the order processing to the entity that sent the order to the centraliser and the UCI.

UCI liability position keeping in France, which should be distinguished from issuance account keeping[44], is therefore always deducted from all of the flows and is neither standardised nor regulated. It is carried out either by the AMC itself, the centraliser or a third party.

UCI liability position keeping is the breakdown of the number of units that are not in registered form per investor or per intermediary in cooperation with the investor – distributor or custody account keeper.

In France, the marking system for subscription and redemption orders for UCI units, allowing for the breakdown in flows, is not mandatory, but has been recommended by the French Asset Management Association (Association Française de la Gestion Financière - **AFG**) and the French Association of Securities Professionals (Association française des

[43] Articles 411-65 and 422-43 of the AMF General Regulation
[44] Issuance account management is defined in Articles 411-70 and 422-48 of the AMF General Regulation

Professionnels des Titres - **AFTI**) for almost 10 years. This marking, which is free of charge, is standardised via a SWIFT codification.

This model involves the appointment of a centraliser responsible for collecting subscription and redemption orders and for executing them on behalf of the UCI[45]. As the UCI units at Euroclear France are bearer securities, the centraliser does not know the identity of the end investor.

There is no share register for a UCI[46] but only an issuance account managed by the issuance account keeper and held at Euroclear France. This issuance account reflects the total number of units on the market.

On the French circuit of subscriptions/ redemptions, 3 organisations are widely used for the same process:

- The AMC is also the centraliser, position keeper and account keeper;
- The AMC is only the position keeper; or
- The centraliser is also position keeper and issuance account keeper.

FOR THE ASSET MANAGEMENT COMPANY	
Advantages of the CSD model	**Disadvantages of the CSD model**
- Low probability of error with delivery against payment **- Low cost because the model is not specific to the fund but to all financial transactions, resulting in considerable economies of scale** **- Possibility of using the funds in collateral management** **- Use of international codes (BIC, BIC1)** **- Flexibility of marking making it possible to identify the entity sought by the AMC**	- Knowledge of UCI liabilities is approximate - There is not always consistency between the statements of position and the order marking - Difficulty in identifying the transfers of position of an investor between two CAK, due to the lack of order marking or investor knowledge

FOR THE INTERNATIONAL INVESTOR	
Advantages of the CSD model	**Disadvantages of the CSD model**
- Low probability of error with delivery against payment **- Flexibility of the model with the option to accept direct orders** **- An investor with a securities account in France can amalgamate all its assets subject to custody fees.**	- Obligation to have a securities and cash account in a bank affiliated with the central depository, Euroclear France - System open to non-French banks, which can become members of Euroclear France but, in practice, mostly domestic banks.

The French model is therefore predominantly a banking one: system for settlement and delivery of fund units or shares, and account management of both the funds' assets and liabilities. In fact, it is based on the CSD system, which only the banks are members of, so all of the finance flows go through these banks.

Similarly, accounts are managed by banking institutions, contrary to the Luxembourg system. In practice, the French model requires fund subscribers to have a securities account in a bank which itself directly or indirectly has an account with the CSD. This model does not make it possible to easily identify distributors and investors, which makes it more complex for the AMC to monitor distributors and to manage the sharing of trailer fees.

For settlements and deliveries and fund liabilities account management, there are considerable disparities between processes. Each subscription may go through several successive settlements and deliveries and several account entries.

Account entries of flows of subscriptions and redemptions do not always allow for identification of the ultimate beneficiary. Intermediaries sometimes aggregate the flows which misrepresents the quality of the marking of the beneficiary's identity.

The marking of subscription and redemption orders means revealing to intermediaries who the AMC's customers are, as marking via BIC/BIC1 formally identifies the legal entity responsible for the subscription or redemption.

[45] *Gestion du passif des OPC et enjeux réglementaires (UCI liability management and regulatory implications), Kramer Levin, July 2014*
[46] *In the event of directly registered shares, a share register may be kept for a UCI.*

In short, the CSD model is based on a system identical to the funds' assets and liabilities, while the needs are very different: additional information is necessary on liabilities (identity of the counterparty) which is lost by the clearing systems.

4.2. The Transfer Agent model

In Luxembourg for example, funds administration includes the function of transfer agent, the main responsibility of which is to keep a register of units of the funds (UCI). This register keeping is regulated but the codifications are neither standardised nor consistent for the same investor.

No centraliser therefore intervenes, as this role is performed by the transfer agent. The latter has an extended scope of activity including:

- processing subscriptions and redemptions and converting the units of the fund;
- checking the identity of the unitholders and the source of the funds invested by them;
- supervising inflows;
- keeping a register of some of the fund's unitholders and of any transfer of ownership of the fund's units. It should be noted that some unitholders are not identified in the register, which then uses omnibus accounts, especially for unitholders whose units are delivered via CSD such as Euroclear or Clearstream;
- monitoring transactions and identifying suspicious or criminal transactions;
- supervising the despatch of statements, reports, opinions and other documents intended for the fund's unitholders;
- managing all the events for the units issued by the fund: distribution or reinvestment of dividends, merger of funds or sub-funds, etc.; and
- calculating and paying trailer fees to distributors.

The transfer agent keeps the official UCI register and is the only entity authorised to collect, process and confirm orders[47]. After the TA confirms the order, the customer or its representative entity gives the instruction to its bank to credit the fund account. Furthermore, this account is usually managed by the UCI depository. In some cases, the transfer agent may keep dedicated accounts at an intermediary bank. In any case, the TA is the only one to reconcile the cash flows with the transactions it has executed.

FOR THE ASSET MANAGEMENT COMPANY	
Advantages of the TA model	**Disadvantages of the TA model**
- Knowledge of UCI liabilities for TA account investors **- Information on the identification of flows and confirmed by statements of position**	- Incomplete knowledge of liabilities when the investors are intermediated - No alignment of procedures - Higher costs - As many registrations as there are TA - Very difficult connection for collateral management - Inflexibility of the register
FOR THE INTERNATIONAL INVESTOR	
Advantages of the TA model	**Disadvantages of the TA model**
- Quick and easy opening of a securities account **- Responsibility for position keeping with the TA** **- Constitutes an historical Benchmark** **- No banking intermediation**	- As many securities accounts as there are TA - Little or no alignment of procedures - Higher costs - More onerous KYC procedure in the event of multiple TA

5. Blockchain, settlement and delivery and account management

Generally speaking, DLT could replace the majority of centralised "trusted third parties" – banks, clearing agents, notaries, land register, etc. – with distributed computer systems.

For example, in order to perform financial transactions, banks currently go through central counterparty clearing houses **(CCP)**. These are trusted third parties that verify the lawfulness of a transaction. They also check that the purchaser actually receives its title of ownership and the vendor the sums due in this respect.

While their guarantee function is crucial in a transaction, CCP continue to be complex and centralised systems. For example, a complex transaction concerning futures markets can take up to two days to clear completely. With a blockchain,

[47] *Gestion du passif des OPC et enjeux réglementaires (UCI liability management and regulatory implications), Kramer Levin, July 2014*

this time limit is considerably reduced to around ten minutes. As the system is automated, the blockchain might also make it possible to completely dispense with certain financial intermediaries such as CCP.

This system would remove the current conflict between CSD model and TA model and have a cross-functional and consistent organisation irrespective of the jurisdiction of the fund of the AMC or investor.

Source: Fundsquare

The advantage is therefore twofold for AMC:

- Transactions completed via a blockchain are more reliable, as they are mathematically secured thanks to a tamper-proof algorithm. The risk of error attributable to the trusted third party, which ceases to exist, is therefore avoided; and
- The absence of the trusted third party mechanically reduces costs, in this case the fees received by the latter.

Whatever the infrastructure model (private or public blockchain) keeping intermediaries in place or not, consideration should be given to the ledger distributed as a ledger common to all banks, generating massive economies of scale and reducing even further the unit costs per transaction.

The blockchain could provide security, confidentiality and customer identification at a competitive cost. DLT would make it possible to dispense with intermediation to establish secure information between two parties.

This system identifies the validity of the flows and the Decentralised Ledger Platform **(DLP)** and records the details of the transactions block by block.

At this stage, a public distributed ledger for management of subscriptions/redemptions would allow access to a number of stakeholders. AMC and investors could join this system directly without necessarily being required to go through a banking institution that manages securities accounts.

However, some issues must necessarily be addressed prior to any use of DLT:

- As the blockchain information is anonymised, it will be necessary to provide identification keys in order to reallocate the event history to the relevant legal entities;
- The information exchanged in the blockchain must be standardised if not normalised to be fit for purpose, including over long periods – a multitude of standards would obstruct economies of scale – irrespective of the DLT used; and
- So that the management of securities accounts via a blockchain guarantees a satisfactory level of security, the law should recognise the methods of registration and custody.

Once these issues are addressed, the advantages for an AMC are as follows:

- The AMC could have detailed and consistent information on all of its funds' liabilities without using the centraliser or the securities account keeper;
- This could herald a multitude of services for fund investors as they are known and traced.

The technological and regulatory issues yet to be dealt with are therefore as follows:

- Compatibility of the use of DLT with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation – **GDPR**) applicable as of 25 May 2018. This issue is further discussed below;
- Recognition or otherwise of cryptocurrencies by central banks or recognition of the token as a method of payment;

- Who would be the trusted third party in a public blockchain?
- What criterion could be used to determine the ownership of a security processed within a distributed ledger?

E. RECORD KEEPING ACTIVITIES

1. General context of record keeping

In contrast to post-trading activities, securities which are not submitted to the operations of a central depository and not issued by a company through a public offering are not subject to custody account keeping and management by an authorised intermediary. These securities are therefore recorded by the issuing company[48] in a register of registered securities holders. When they are issued by a collective investment fund, the securities are recorded as 'account issuance' of stocks or shares.[49]

Although it is not custody account keeping, the recording of securities in the name of their holders in registers held by issuers, mutual funds or their representatives is made in 'securities accounts'[50].

The securities concerned are not intended to lose their registered status: only those securities submitted to the operations of a central depository may circulate in the bearer form, subject to the leeway allowed in article L. 211-7 of the Monetary and Financial Code for collective investment fund units and shares.

The owner of registered financial securities may engage an authorised intermediary as custody account keeper to manage their securities account with an issuer. The securities then take the form of administered registered securities.[51] In this latter case, once the mutual fund's units or shares circulate in the form of both registered and bearer, a reconciliation of the securities is necessary.

2. Professional rules for record keeping

For issuers, their representatives, or custody account keepers to be able to honour their respective obligations, and for the latter to process the operations initiated by issuers or holders of financial instruments in the best conditions, a technical specifications sheet was drawn up under the auspices of the French Committee for the Organisation and Standardisation of the Banking Sector **(CFONB)**.

This specifications sheet, the latest version of which dates from 2013[52], describes the order of standardised transfer, the sole medium of transfer of financial instruments between issuing companies or their representatives and custody account keepers in charge of the administration of administered registered securities accounts. This specifications sheet has a professional regulatory status according to article 322-54 of the French Financial Markets Authority (AMF)'s General Regulations when the securities are issued through public offering.

3. Practical difficulties regarding record keeping

For the account holder, a transfer consists of debiting a certain number of financial instruments from an account and crediting one or several others with the same number. The transfer through a recorded register is performed today in practice by means of a transfer order signed by the transferor, whereby the issuer records the operation as having taken place and proceeds with the registration of the required securities.

The cause for the transfer of securities may be:

- a transfer of ownership, regardless of its form: a sale, a trade, a donation or a contribution,
- a securities transaction: allocation, subscription, etc.
- or a transfer with no change of ownership or any other operation involving a transfer of securities: conversion from pure to administered registered security and vice versa.

The administrative burden involved in processing the transfer of recorded shares is considerable in

[48] Articles R. 228-7 to R. 228-9 of the Trading Code
[49] Articles 411-70 RGAMF (OPCVM) and 422-48 AMF General Regulation (FIA)
[50] Article L. 211-3 of the Monetary and Financial Code
[51] Article R. 211-4 of the Monetary and Financial Code
[52] Cahier des Charges applicable aux teneurs de comptes d'instruments financiers français non admis aux opérations d'un dépositaire central, Communication CFONB n° 2013-0041

the sense that this transfer implies the exchange of several copies of the original document being exchanged between the different parties. Yet, until the book entry has actually been completed, the transfer of property to the assignee has not happened, and the operation is not enforceable against third parties.

These difficulties are even more serious when the securities benefit from, or are subject to, a specific tax regime: Personal Equity Plan (PEA – Plan d'épargne en actions), securities from stock options or the purchase of securities, bonus shares, founder warrants, etc. Yet, transfer orders are not intended to transport fiscal information.

Using the DLT technology may provide security and efficiency for issuers or their representatives, financial intermediaries, custody account keepers, and of course, investors. All the more since the European regulation CSDR of 23 July 2014 relative to central depositories clearly provides for the case of a plurality of depositories, issuers and registrars to put in place 'adequate cooperation and information exchange measures with each other so that the integrity of the issue is maintained'[53].

[53] *REGULATION (EU) No 909/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 Article 37.1 and 37.2:*

FOCUS ON DERIVATIVES

The following section aims to contribute to expanding the discussion on the use of the DLT on derivatives, designated under French law as *"contrats financiers"* or *"instruments financiers à terme"*.

The DLT, an important issue for derivatives

Compared to post-market activities, there were not many DLT applications in the derivatives industry and the DLT was not at the centre of the various reports issued by European regulators or international institutions mentioned hereinafter.

However, the DLT represents a very important issue for derivatives for two main reasons.

First of all, from a structural perspective, derivatives require significant data reconciliation work between the parties to a contract, as the value of the contract depends on the value of underlying assets.

Then, after the 2008 financial crisis, commitments were made at an international level (G20 of Pittsburgh in 2009) to provide better regulation for derivatives. These commitments led to a mandatory reporting of transactions to trade repositories, a clearing obligation for some standardised derivatives and reinforced requirements of collateralisation for non-cleared derivatives (EMIR Regulation[54] in EU), which notably requires the parties to carry out reconciliation work more often.

Since it allows users to stock and access information relating to a given set of assets and to handle transactions which are registered in a network, the DLT should result in a more efficient management by the parties of their derivatives transactions.

Recent applications of DLT to derivatives

Different projects have been launched or are ongoing, even if the public information available relating to these projects remains scarce.

The common features of these various projects lie in the following objectives:

- integrate in an information system shared between the different parties elements which were usually retained in the proprietary information systems of each of the parties to a derivatives transaction; and
- integrate to the extent possible legal aspects directly in the information systems.

Concerning the execution of transactions on a blockchain, the project[55] consisted in integrating in a *smart contract* crucial information on a basic derivative operation, and then executing this transaction on a blockchain. The operation implied flows during its inception, development and conclusion. The project was carried out on the consortium R3's platform.

Management of events affecting the underlying assets during the life of the transaction: *the Depository Trust and Clearing Corporation* **(DTCC)** launched at the beginning of 2017 a project to revamp the *Trade Information Warehouse* **(TIW)** based on the principle of blockchain. TIW helps both collecting information on derivatives transactions and managing *post-trading* events affecting the underlying assets of credit derivatives. The governance will be provided by DTCC and the companies that would be members of TIW would each have a copy of the distributed ledger.

The main challenges when implementing blockchain projects applied to derivatives appear to consist of:

- the need to be able to gather a sufficient number of counterparties so that the network can acquire a critical mass;
- the degree of maturity of current blockchain platforms; and
- the integration of these blockchains with existing computer systems in financial institutions.

ISDA and the development of smart contracts

The use of blockchain would support the effort of standardisation of the documentation implemented by the International Swap and Derivatives Association **(ISDA)**.

1. A CSD shall take appropriate reconciliation measures to verify that the number of securities making up a securities issue or part of a securities issue submitted to the CSD is equal to the sum of securities recorded on the securities accounts of the participants of the securities settlement system operated by the CSD and, where relevant, on owner accounts maintained by the CSD. Such reconciliation measures shall be conducted at least daily.

2. Where appropriate and if other entities are involved in the reconciliation process for a certain securities issue, such as the issuer, registrars, issuance agents, transfer agents, common depositories, other CSDs or other entities, the CSD and any such entities shall organise adequate cooperation and information exchange measures with each other so that the integrity of the issue is maintained.

[54] REGULATION (EU) No 648/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 4 July 2012.

[55] Project led in particular by Barclays in April 2016.

It should be noted that ISDA was created with a view to maximising the standardisation of OTC derivatives operations in order to facilitate the negotiation of transactions between parties and the management of these transactions. This historical goal was recently recalled through a publication dated September 2016[56] where the ISDA reasserted its ambition to integrate at a maximum level technological evolutions to derivatives, taking into account in particular the increased amount of regulation.

The recent publication in August 2017[57] of a whitepaper questioning the contribution of the DLT and *smart contracts* to derivatives is therefore part of the fundamental trend aimed at standardising, as much as possible, the documentation of these products.

A blockchain applied to derivatives would work in the following way: the blockchain, which is private, would be open only to participant members and the transactions would be registered in this distributed ledger. A *smart contract* deployed over the network would automatically carry out some actions relating to certain transactions.

Legal contracts and computer code

This white paper focuses on interesting issues primarily concerning the question of the point at which a contract can be coded. The conclusion is that it is not possible for a legal contract to be completely coded and performed on a blockchain. This justifies the proposed distinction between the "smart legal contract", a legal agreement between the parties (which can integrate computer code), and the "smart contract code", the computer code directly executable on the blockchain.

It appears that at best the "smart contract code" could replace certain operational clauses of the contract of the derivative transaction. If this is not possible, the "smart contract code" could be just a way to automatize already existing terms of the contract. Among operational terms which would be easily transferable into a *smart contract code*, we would find for instance terms stating that a payment has to be done at a given date – for example the pay-off of an option. Among non-operational terms that could not be transferable into a *smart contract code*, we would find for instance those stating the applicable law of the contract between the parties, the choice of applicable jurisdiction in case of litigation, or even statements issued by the parties.

Supporting the development of the smart contract code would require significant work on the re-formalisation of the ISDA definitions. Furthermore, the difficulty with automating everything is that it is possible for both parties to make certain choices during the transaction – for instance, if a termination event occurs, one of the parties can decide whether it will exercise this right during a certain period of time, which in principle appears to be non-programmable.

However, whilst information outside of the contract is necessary for the implementation of the computer code, they could be replaced by determinations of third-party oracles – for instance for a credit default swap (CDS), a determination of the Credit Derivatives Determinations Committee in order to allow for the continuation of the execution of the computer programme.

[56] *The future of derivatives processing and market infrastructure, ISDA Whitepaper, September 2016.*
[57] *"Smart contracts and Distributed ledger – a legal perspective", ISDA and Linklaters, 3 August 2017.*

FOCUS ON THE CAISSE DES DÉPÔTS

As the historic public trusted third party in France, the Caisse des Dépôts started investigating DLTs very early on, starting its Blockchain Programs and launching LaBChain in 2015. LaBChain is the first European consortium dedicated to the collective exploration of DLTs and blockchain use cases in the banking finance and insurance sector, federating 31 financial, technological and institutional members today.

With its "techno-agnostic" approach - since it is open to any kind of protocol and technology - the Caisse des Dépôts has the ambition to use blockchain as a digital public infrastructure to improve the resiliency, transparency and efficiency of existing financial systems while creating new services to support the French ecosystem and serve the citizens.

In collaboration with the financial and blockchain startup ecosystem in France, the Caisse des Dépôts is committed to the development of numerous experimentations on a vast array of blockchain use cases. While fueling the research and development operations of the institution, this innovation process contributes to the exploration of the technology's functionalities, benefits and limits and to the dialog with other public institutions, with the regulator and the legislator to identify the legal challenges of DLTs and their future.

Beyond the dozen of strategic blockchain projects currently ongoing within the Caisse des Dépôts and its many subsidiaries, the Caisse des Dépôts experiments blockchain in the financial sector with LaBChain consortium, especially in the management of securities lending for non-cash collateral, digital identity and KYC processes. Those experimentations are also furthered through a partnership with the technical research institute IRT SystemX, delivering high-level research on its dedicated FinTech-RegTech platform.

Furthermore, the Caisse des Dépôts also initiated with its partners BNP Paribas, CACEIS, Euroclear, Euronext, S2iEM, Société Générale, and with the support of Paris Europlace, the creation of LiquidShare. LiquidShare is a new European FinTech startup using DLTs to simplify and speed up the post-trading operations for unlisted SMEs while reducing transaction and infrastructure cost.

Finally, following the executive order issued on the 28th of April 2016, dedicated to the reform of the legal status of over-the-counter bonds ("bons de caisse"), the Caisse des Dépôts is developing, in collaboration with the crowdfunding association Finance Participative France and several of its members, a blockchain infrastructure to issue, record and exchange "minibons". After a successful prototype, the Caisse des Dépôts and its partners are getting ready to move on to the production phase before the end of 2018.

III. THE INTERNATIONAL REGULATORY ENVIRONMENT OF THE BLOCKCHAIN

The success of the blockchain and the development of crypto-currencies has not left European or international regulators and institutions indifferent; they have each contributed to the general reflection by publishing many studies, or even proposing a reflection for an adequate regulatory framework for its development.

Although the regulators were reserved or even hostile to Bitcoin, they take an entirely different view of DLT. Indeed, the regulators welcome this new technology, seen as a way to improve the security and efficiency of financial markets.

A. POSITIONS OF THE EUROPEAN INSTITUTIONS AND REGULATORS

1. European Securities and Markets Authority (ESMA)

The European Securities and Markets Authority **(ESMA)** has already published three documents relating to DLT: a call for papers[58], a consultation document[59] and a report on the application of DLT to financial markets[60].

These three documents reveal ESMA's keen interest in the development of the blockchain. Aware of the stakes and the technical nature of the subject, the authority wished to conduct a reflection by encouraging the active participation of the public in its approach. The call for papers of April 22, 2015 demonstrates the need for regulators to learn more about a technology they know little about. Therefore, the aim of the European Regulatory Authority was, first and foremost, to collect as much information as possible to understand the risks and benefits of the technology in order to determine, where appropriate, whether or not to legislate on this matter.

Above all, ESMA sees in DLT the means to significantly reduce the structural costs of market transactions and to develop financial exchanges in the securities sector.

However, for ESMA, DLT is more of a tool for reducing transaction costs than a revolutionary instrument for rebuilding the architecture of the market.

It is in post-trading activities that ESMA recognises the strongest potential of the DLT. In an effort to highlight the difficulties of implementing distributed registries, particularly with new entrants, the authority identifies the main issues to be resolved before considering the large-scale expansion of the technology:

- The need for interoperability with existing infrastructures;
- Access to central bank money;
- Governance of systems;
- Protection of data entered on shared registers; and
- Without departing from the law as it stands, the risks of the application of European legislation to blockchain systems.

It is also important to note that ESMA does not consider that current law prevents the development of the technology. At most, certain provisions should be clarified to facilitate its operation, in financial law as well as in company, contracts, insolvency or competition law.

[58] *Call for papers of April 22, 2015 available at the following address: https://www.esma.europa.eu/sites/default/files/library/2015/11/2015532_call_for_evidence_on_virtual_currency_investment.pdf*
[59] *Consultation document of June 2, 2016 available at the following address: https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf*
[60] *Report of February 7, 2017 available at the following address: https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf*

2. European Central Bank (ECB)

In April 2016, the European Central Bank published an occasional paper on the blockchain mechanism applied in the post-trading sector[61]. The institution specifies, however, that its content can not reflect its position on DLT. However, this document remains a good indicator of how the ECB perceives the arrival of this new technology.

Like ESMA, the authors see the technology as a decisive means of improving the functioning and attractiveness of financial markets: reducing reconciliation costs, improving the value chain in post-trading, or even a more efficient use of the guarantees granted.

The report also shares ESMA's circumspection about its ability to offer a new market architecture. In particular, the authors believe that the blockchain does not seem able to replace the current clearing houses, especially in the framework of clearing futures transactions.

The publication also contains reservations on the capacity of DLT to overcome, in the short term, the difficulties related to its implementation on the markets.

A report from the ECB's Advisory Group on Market Infrastructures for Securities and Collateral **(AMI-SeCo)** published in September 2017[62] discusses in greater detail the various potential practical applications of DLT in terms of market activities, while highlighting the early stage of development of this technology and therefore the difficulty of deciding not only on its large-scale adoption on the financial markets, but also on the type of DLT that could be adopted if necessary.

3. The European Parliament

The European institutions show a growing interest in blockchain. The *European Parliament's Sciences and Technology Option Assessment* **(STOA)** Committee recently decided, in conjunction with the European Commission, to set up a DLT working group to monitor the evolution and operation of this new technology and to determine whether or not there is a need to legislate.

In parallel, in March 2017, the European Commission published a consultation document on Fintechs and, among others, the use of DLT[63].

A recent publication of the European Parliament in February 2017 entitled *"How blockchain could change our lives"*[64] and drafted by its STOA committee was disseminated with the aim of raising the awareness of MEPs on the virtues of this technology. The document broadly outlines the issues surrounding the adoption of a legislative framework for blockchain, without limiting itself to the financial world. This publication therefore has an important place in the design of the future European regulation, since it will constitute one of the bases to guide the work of the MPs. While the report is enthusiastic about the large-scale development of blockchain, it remains cautious about its revolutionary aspect.

B. INTERNATIONAL INSTITUTIONS

1. Financial Stability Board (FSB)

In a speech delivered on November 3, 2016 at a conference[65], the FSB Secretary General, Mr. Svein Andresen, said that the organisation had initiated a discussion on the regulation of DLT in order to offer regulators a series of recommendations in this area.

This work is being conducted in parallel with the Payments and Market Infrastructures Committee to identify the key points that will be addressed by the Member countries.

2. Bank for Intervnational Settlements (BIS)

The Payment and Market Infrastructures Committee of the Bank for International Settlements published, in February 2017, an analytical report on DLT in payment, clearing and settlement services[66].

This report offers national regulators as well as central banks a grid that analyses and helps

[61] *Available at the following address: https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf*
[62] *The potential impact of DLTs on securities post-trading harmonisation and on the wider EU financial market integration, BCE, Advisory Group on Market Infrastructures for Securities and Collateral, September 2017*
[63] *Available at the following address: https://ec.europa.eu/info/sites/info/files/2017-fintech-consultation-document_en_0.pdf*
[64] *Available at the following address: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf*
[65] *Available at the following address: http://www.fsb.org/wp-content/uploads/Chatham-House-The-Banking-Revolution-Conference.pdf*
[66] *Available at the following address: http://www.bis.org/cpmi/publ/d157.pdf*

understand the technology, in order to set out the risks and opportunities of its implementation. Recalling the rules and possible uses of the blockchain registry, the report again emphasises the immature nature of the technology and the lack of real revolutionary potential on the current market infrastructure.

In September 2017, the BIS also published a long study on cryptocurrencies in its quarterly report[67]. The study looks in particular at *central bank cryptocurrencies* **(CBCC)**, cryptocurrencies issued by the central banks and exchanged on a decentralised peer-to-peer network. The BIS distinguishes between two potential forms of CBCC, the first being a widely accessible payment instrument for consumers *(retail CBCC)* and the second a restricted access token for wholesale payments *(wholesale CBCC)*. While the first would guarantee consumers the anonymity of their payments as is already done by fiat money, the second would mean a reduction in transfer costs. The study also highlights some potential risks associated with the development of CBCC, including the incitement to bank runs if the bank money is easily exchangeable against CBCC without risk and damage to the business model of credit institutions.

3. International Organization of Securities Commissions (IOSCO)

In a report on Fintechs[68], IOSCO develops its vision for the use of DLT as well as possible regulatory framework solutions.

It should be noted that IOSCO remains cautious in the use that can be made of it. As such, the organization recalls in its report the circumstances of the attack on The DAO and highlights the risks associated with maintaining a single decentralised registry. While DLT globally reduces the share of human error in the functioning of a market infrastructure, it also aggravates the consequences of coding errors.

IOSCO calls first and foremost for greater cooperation among regulators, all the more important as DLT is in essence an international phenomenon, subject to resulting in the accumulation of applicable regulations and supervisory bodies.

4. International Monetary Fund (IMF)

The IMF has published two reports on the DLT:

- A report on cryptocurrencies published in January 2016[69]; and
- A report on Fintechs and financial services published in June 2017[70].

The first report details the emergence of cryptocurrencies and DLT, highlighting the regulatory challenges raised by these technological innovations. The IMF highlights the difficulties posed by anonymity in the fight against money laundering, fight against the financing of terrorism, fiscal policy and exchange control. It also highlights the protection of consumer interests against fraudulent transactions based on DLT and cryptocurrencies.

The second report explores the potential innovations of Fintechs in terms of transaction security, confidence in the financial markets, protection of anonymity and improvement of financial services. The IMF concluded that it is difficult to anticipate the extent of the evolutions caused by Fintechs in the years to come. As such, it urges national regulators to exercise caution in order to maintain the integrity and stability of financial markets, especially in the fight against money laundering and the financing of terrorism, cybersecurity and data integrity, algorithms and platforms.

[67] *BIS, Central bank cryptocurrencies, September 2017: https://www.bis.org/publ/qtrpdf/r_qt1709f.htm*
[68] *Available at the following address: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf*
[69] *Virtual Currencies and Beyond: Initial Considerations, IMF Staff Discussion Note, January 2016*
[70] *Fintech and Financial Services:Initial Considerations, IMF Staff Discussion Note, June 2017, available at the following address: http://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2017/06/16/Fintech-and-Financial-Services-Initial-Considerations-44985*

IV. THE LEGAL QUESTIONS RAISED BY BLOCKCHAIN IN THE AREA OF FINANCIAL INSTRUMENTS

DLT can directly impact the legal regime of financial instruments by calling into question the mode of holding, the transfer of ownership regime, but also more fundamentally the mode of representation of securities, with the concept of "e-securities". However, legal studies in Europe on the impact of this technology are rare.

The impacts of DLT, however, do not stop at securities law. Beyond the legal regime specific to financial instruments, this technology raises questions for the jurist on many other aspects: law of evidence, intellectual property law, protection of personal data, cybersecurity, etc. All these questions are not specific to securities law but should be examined to see if and how they can impact the use of blockchain in post-trade activities.

The legal challenge posed by DLT is to evaluate to what it extent it upsets the traditional legal concepts and, depending on the case, the need or not to extensively reform some branches of the law in order to adapt it to this technology. The issue needs to be examined both in the cross-cutting areas of law such as intellectual property, data protection, electronic signature and cybersecurity, as well as in the more specific law governing post-trade activities.

At this stage of reflection, DLT does not prove to be so incompatible with the existing legal framework that it would be necessary to create a new branch of law specific to this technology. On the contrary, common law makes it possible to convincingly deal with most of the issues raised by this technology. While some adaptations may be necessary, especially for taking into account the ownership regime of securities registered in a blockchain, it is more of question of clarification than substantial changes.

The following are simple indications and do not constitute a detailed legal analysis of the impacts of this technology on the rules of law that govern any particular area of law.

A. BLOCKCHAIN AND SECURITIES LAW

If, as discussed in the above section on tokens, DLT is likely to change the legal concept of financial security in itself, it could also influence the legal regime of the representation of financial securities.

The following developments relate more specifically to unlisted securities, and not shares and units of UCIs that also comply with a specific regime, as discussed above.

The practice of securities custody / accounting differs schematically between direct holding systems and indirect or multi-intermediated holding systems. In the same way, the principle of book-entry is the usual mode of operation in the financial markets, whether in direct or indirect holding systems, even if in some countries securities are still materialised or represented in the form of a global certificate. Thus, with regard to the circulation of securities, as in the case of proof of holding the right on securities, registration in the name of the holder (whether the owner or an intermediary in the case of a chain of custody) plays a central role in the rights of the holder. The difficulty with using a DLT is that the concepts of central registry or accounts are no longer relevant. How then can the enforceability of rights be ensured in a DLT? In fact, everything depends on the role of the DLT. If it only reflects the book entries, then it is only a technology with no influence on the legal regime of securities; if, on the contrary, all the securities issued by an issuer are placed in a DLT and the purchases and sales of these securities can only be made via this DLT, then it takes on another dimension.

It is in this sense that it is first necessary to examine the conditions under which securities may circulate in a DLT under European law, in particular the Central Securities Depository Regulation ("**CSDR**")[71].

[71] *Regulation 909/2014 of the European Parliament and of the Council of July 23, 2014 on central securities depositories.*

DLT and Central Securities Depositories:

The admission of a financial security to the operations of a CSD, or its delivery into a settlement and delivery system for financial instruments, results either from a regulatory constraint or from the choice of the issuer or owner of the financial security.

Firstly, certain financial securities are compulsorily admitted to the operations of a CSD under European law. Article 3(2) of the CSDR Regulation provides that:

> *"Where a **transaction in transferable** securities takes place on a trading venue the relevant securities shall be recorded in book-entry form in a CSD on or before the intended settlement date, unless they have already been so recorded.*
>
> *"Where transferable securities are transferred following a financial collateral arrangement as defined in point (a) of Article 2(1) of Directive 2002/47/EC, those securities shall be recorded in book-entry form in a CSD on or before the intended settlement date, unless they have already been so recorded."*

The CSDR is based on the definition of "transferable securities" used in the MIF2 Directive[72], which covers "classes of securities which are negotiable on the capital market" a non-exhaustive list of which is given by the Directive, including company shares, bonds and other debt securities. However, Section C of Annex I of the MIF 2 Directive clearly distinguishes, among the categories of financial instruments, transferable securities from money market instruments and units or shares of undertakings for collective investment.

Then, certain financial securities are obligatorily admitted to the operations of a CSD. French law does not restrict this scope. Indeed, Article L.211-7 of the Monetary and Financial Code does not require registration with a CSD and leaves the choice to the issuer to carry out custody account keeping.

Under French law, financial instruments are defined as securities and contracts:

> *"II. - Financial securities are:*
>
> *1. Capital securities issued by corporations;*
>
> *2. Debt securities;*
>
> *3. Units or shares of undertakings for collective investment.*
>
> *III. - Financial contracts, also known as "forward financial instruments", are futures contracts that appear on a list fixed by decree.*
>
> *IV. - Commercial papers and cash certificates are not financial instruments[73]".*

In this definition, financial instruments in the form of securities - equities and equity securities, but also bonds and debt securities - should be distinguished from those in the form of financial contracts - swaps, options and other futures contracts. Only the category of securities has been studied in this report.

Dematerialized since 1984, financial instruments in the form of securities are now only represented by a book entry. This concept of book entry has since flourished since it is considered at the international level as the summa *divisio* in the area of securities, to differentiate them from financial instruments that remain represented in paper form or by certificates.

French law distinguishes between registered securities and bearer securities, the first being registered in an account with the issuer while the second are registered in an account with an authorised financial intermediary.

As can be seen, the concepts of account and that of account holding are central in the French conception of securities law. To such an extent to link the transfer of ownership to the registration in an account: according to Article L. 211-17 of the Monetary and Financial Code, *"Transfer of ownership of financial securities results from the registration of these securities in the purchaser's securities account".*

This concept of ownership as an absolute right of the investor vis-à-vis the issuer of the financial instrument is a cornerstone of the French conception of securities law. It can be summarised around three principles:

- Right to the ownership of securities registered in an account: the person registered in the account is the sole owner of the securities and in any case, he has an exclusive right on the securities registered in the account opened in his name. No competing claim can be made. Although these securities are fungible, the account holder is not the owner of these securities at any level of the chain of custody.

[72] *Directive no. 2014/65/EU of the Parliament and of the Council of May 15, 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.*
[73] *Article L. 211-1 of the Monetary and Financial Code*

If the account is closed, it must return the same securities for the same quantity;

- Uniqueness of the securities account of the owner: there is only one account that is authentic, that is to say that testifies to the ownership of the securities exclusively in favour of the account holder, whether with the intermediary, or the issuer. The other accounts are mirror accounts, whether in the intermediation chain or with the central depository;
- Securities accounting by debit-credit: any transfer of ownership of securities must result in a debit and credit on two different accounts.

The problem with DLT is that it has no *account*: after entries in a decentralised account, this technology does not work by debiting one account and crediting another, but as a sequence of transactions.

It is in this sense that this technology potentially changes the world of securities law, not only in France but in all countries that use the concept of *book entry securities*. In fact, two international conventions on securities law put this concept at the heart of their objective:

- the Hague Convention of July 5, 2006 on the law applicable to certain rights in respect of securities held with an intermediary; and
- the Unidroit Geneva Convention of October 9, 2009 on material rules relating to intermediated securities.

In French positive law, the representation of financial securities is performed by means of their registration in an account in the name of their owner.

As provided for in Article L.211-3 of the Monetary and Financial Code, *"financial securities, issued on the French territory and subject to French legislation, are registered in a securities account held either by the issuer, or by one of the intermediaries mentioned in 2° to 7° of Article L.542-1"*.

Article L.211-4 states that this registration is carried out *"in the name of one or more holders, owners of the financial securities registered in the account"*, subject to exemptions (registered intermediaries, in particular).

Article L.211-8 of the Monetary and Financial Code allows the custodian account keeper to delegate its tasks to a third party.

The current system of representation and transmission of unlisted securities:

The system for the representation and transmission of unlisted financial securities (*i.e.*, not admitted to the operations of a central depository or delivered in a system for the settlement and delivery of financial instruments) operates in practice according to the following diagram.

Firstly, an unlisted company has a book titled "Share Transfer Register" in which all operations relating to the securities of the company concerned are transcribed (issues, capital increases, transfers, pledges, etc.). It is a kind of "log book", traditionally numbered and initialled by the registry of the Commercial Court with which the company is registered, without this being a formal condition of validity[74]. Secondly, an unlisted company keeps an "issue" account that tracks all of the company's issues of securities and the volume of securities issued by the company; this account, which is structurally debtor, is only active during capital transactions and always represents the total amount of securities issued. Finally, in accordance with Articles L. 211-3 et *seq*. of the Monetary and Financial Code, the company or its appointed agent (whose name and address must be published in the Bulletin of mandatory legal announcements in accordance with Article R. 211-3 of the Monetary and Financial Code) must keep "registration accounts" or "holders' accounts" in the name of each of the shareholders in which the financial securities they own are registered[75].

On the legal level, holders' accounts are the "securities accounts" referred to in Article L. 211-3 of the Monetary and Financial Code. These securities accounts are fundamental for the registration of securities, the verification of ownership rights and the recognition of transfer of ownership transactions. Article R. 211-1 of the Monetary and Financial Code stipulates that *"financial securities are only materialized by a registration in the account of their owner"*. It is thus the registration in an account which materializes the security and establishes the shareholder's right of ownership over the security. Furthermore, Article L. 211-17 paragraph 1 of the Monetary and Financial Code states that the transfer of ownership of securities results from the inclusion of these securities in the securities account of their purchaser, these transfers being operated by transfer from one shareholder account to another (Article L. 211-15 of the Monetary and Financial Code). Regarding unlisted financial securities[76], the

[74] Cf. Written question no. 01986 of Mr. Lucien Neuwirth (Loire - RPR) published in the OJ Sénat of 10/07/1986 - page 951

[75] In accordance with Article L. 212-3 I of the Monetary and Financial Code, shares issued in France and subject to French law that are not admitted to trading on a regulated market must, in principle, be in registered form (except in case of an exception applicable to certain investment vehicles).

Commercial Code also specifies that the registration in the account of the purchaser is done on the date fixed by agreement of the parties and notified to the issuing company[77].

Accordingly, registration in the account also constitutes the key element to record the existence and ownership of unlisted financial securities and the ownership transfer transactions on these securities (which can also be documented by the share transfer register).

In practice, transfers of ownership of unlisted securities are now effected by means of share transfer orders signed by the transferor[78] in view of which the issuing company records the transaction[79], enters it in its share transfer register[80] then finally transfers the securities from the transferor's securities account to that of the transferee[81].

Share transfer orders are not subject to any particular formalism for transfers of unlisted financial securities. Nevertheless, in practice, share transfer orders are based on the order model annexed to the Afnor NF K 12-500 standard. They specify in particular the nature of the securities that are the object of the sale (capital shares, dividend shares, convertible bonds, etc.), the par value of the securities[82], the terms of the transaction (registration in an account, transfer, redemption, transmission, donation, subscription, pledge, etc.)

Still on the practical level, shareholders' accounts are usually established in the form of single sheets (generally drawn up on one side only) reserved for a holder of securities on the basis of his ownership or for several holders by reason of their co-ownership, their lease, their bare ownership or their usufruct on these securities.

For each financial securities transfer operation, based on the share transfer orders transmitted to it[83], the issuing company enters in the share transfer register in chronological order: (i) the date of the transfer of ownership transaction, (ii) the surnames, forenames and address of the former and new holder of the securities (or the company name, identification number and registered office for legal persons), it being specified that the name of the former holder of the securities may be replaced by a serial number allowing this name to be found in the registers, (iii) the par value and the number of securities transferred (however, where these securities are shares, the share capital and the number of securities represented by all the shares of the same class may be indicated instead of their par value), (iv) if applicable, if the company has issued shares of different classes and there is only one registered share account per shareholder, the category and characteristics of the shares transferred and (v) the order number assigned to the transaction[84].

Special provisions also apply to pledges of unlisted securities. In the case of pledge transactions, the name of the holder of the shares must be indicated with the words *"Securities pledged in favour of (identity of the person concerned)"*.

The failure to keep the share transfer register of an unlisted company and shareholders' accounts is not sanctioned by the texts. Nevertheless, with regard to the above-mentioned texts, the non-registration of financial securities in an account and the recording of account-to-account transfers materialising the transfers of these securities would pose major problems in ascertaining the rights of shareholders and could incur the civil liability of the issuer, in particular vis-à-vis the purchaser.

In view of these elements, although there are three levels of registration of securities and/or transactions on securities issued by an unlisted company, it is in fact only the securities accounts in which the entries appear that "represent" the financial securities and which make it possible to ascertain the ownership rights of the account holders.

Functions of a DLT:

In this context, three functions can be assigned to the DLT.

- Alternative technology to the keeping of securities accounts: the securities would continue to be registered in a securities

[76] Article L. 228-1 of the Commercial Code specifies that securities are financial securities within the meaning of Article L. 211-1 of the Monetary and Financial Code, which confer identical rights by category.
[77] Article R. 228-10 of the Commercial Code.
[78] The obligation to sign is the sole responsibility of the transferor who fulfils by this signature his obligation to deliver the shares transferred. This obligation was confirmed by a judgement of the Commercial Division of the Court of Cassation on May 24, 2011 (Court of Cassation, Commercial Division, May 24, 2011, no. 10-12163).
[79] Article R. 228-8 of the Commercial Code with regard to securities.
[80] As regards the information to be given on the register, cf. Article R. 228-10 of the Commercial Code and Article 4.2 of the aforementioned CFONB specifications.
[81] As regards the information to be given on the holders' accounts, cf. Article 4.3 of the aforementioned CFONB specifications.
[82] The following information is also added for bonds: the year of issue and the applicable interest rate.
[83] It is considered that by signing the share transfer order, the transferor instructs the issuing company to debit his shareholder account and correlatively to credit that of the transferee for the number of securities indicated in this transfer order.
[84] Article R. 228-9 of the Commercial Code as regards securities and Article 4.2 of the aforementioned CFONB specifications

account opened in the name of the owner of the securities, and the DLT would be used either as a substitute for traditional securities account keeping technologies (i.e., operationally, the securities accounts would be included in the DLT) or as an addition to the securities account keeping technologies (i.e., operationally, the DLT and securities accounts would be separate, the DLT being used primarily for reconciliations between securities accounts and the transmission of securities - see next section). Where applicable, the registrations in the DLT could be used in case of default by the account holder to determine how many financial securities are to be returned to the account holders, similar to accounts held by a CSD under Article L.211-10 of the Monetary and Financial Code.

- Proof of ownership of the securities: the securities would continue to be registered in a securities account opened in the name of the owner of the securities, but the registration in the DLT could have the force of proof.
- the financial securities would be represented by a registration in the DLT, either because the registrations in the DLT would be considered as registrations in a securities account, or because the law would expressly provide for this.

The responses to the Treasury's consultation with the financial marketplace during Spring 2017 seemed to indicate that the players wanted to see the use of DLTs in this third option. In such a case, it will therefore be necessary to ensure that registrations in the DLT will have the same effects as those of a registration in an account with an intermediary or the issuer.

One of the solutions would then consist of legally assimilating the registrations in a DLT to book entries.

B. BLOCKCHAIN, INTELLECTUAL PROPERTY LAW AND PATENTS

What are the various components of a blockchain and who are its authors? Can these authors claim any rights on their creations? Practically speaking, how do these rights manifest themselves? The aim of this paragraph is to determine if French intellectual property law is suited to answer these questions relating to new technology.

1. The components and authors of the blockchain

To analyze DLT (Distributed Ledger Technology) from an intellectual property law point of view, we must define the various components and try to identify their authors.

1.1. The components of the blockchain

The software source codes

DLT is nothing more than software programs necessary for a wide range of applications. The most concrete examples are smart contracts, i.e. self-standing programs that, when they run, automatically process pre-established conditions within the blockchain. Blockchain software programs are created through codes, known as "source codes". A software source code is what the programmer uses to build and edit the software program.

Blockchain history or "data"

Blockchain data represents the whole history of movements, all the transactions that occurred on that worldwide network. All of this data is automatically and indefinitely stored in the blockchain as lines of code.

Digital assets or "tokens"

"Tokens" are digital assets the blockchain users own. In this article, we will explain their principles and characteristics.

Software visual interface and blockchain websites

As any website or software program available on the Internet or indeed any digital device, the visual interface of all the sites that give form to the DLT are an integral part of it.

1.2. The authors of blockchain

Public blockchain, private blockchain: web developers, programmers, graphic designers, minors

All blockchains, whether they are public or private, are software programs whose designers - whether they are natural or legal persons - are identifiable. Therefore, the public or private nature of a blockchain should not have any impact on the ownership of source codes, object codes, visual interfaces, etc. that make up these blockchains. In any event, they are, designed by web developers, programmers and graphic designers. Minors - paid or voluntary contributors who manage the blockchain network – do not generate any intellectual property provided they merely implement the codes or interface and do not create or improve them.

The blockchain, author of the blockchain: artificial intelligence

Autonomous work created by blockchain software programs cannot be protected. This solution is not unlike a famous US Court case, where a California Court of law refused to grant copyright to a monkey who had taken selfies.

2. Blockchain, a possible "joint" ownership for public blockchains

2.1. Public and private blockchain: an ineffective distinction

Should we apply the theory of joint ownership to software programs, we could think that the software designer who decides to enable anyone who uses the program to copy, study and even edit it before redistributing it, would give up all of his/her rights on what was created. However, open-source or free software programs can be defined as software *"protected by copyright and usually free of charge - although sometimes against payment - (which) can be run, studied, distributed and edited according to the terms and conditions of a license"*[85].

Consequently, software programs, even open-source software still fall under copyright rules. We must therefore distinguish between open-source licenses and those that belong to the public domain.

2.2. An intellectual property view of "free licenses"

In a public blockchain, the software and its source codes are accessible to all so that the whole community may operate, copy, distribute and even edit them to improve the performance of the software.

Therefore, the blockchain original protocol and all its implementations – including Ethereum – are protected by the GNU General Public License v2, a "reciprocal" open-source license that sets up a legal framework for the use and editing of the protected programs. Consequently, the right to edit and redistribute is guaranteed only if the user provides the modified version of the software. Additionally, the distributed copies, including their modifications, must also comply with the terms of the "GPL" (General Public License)[86].

While these licenses are often used in public blockchains, it is less true of private blockchains, for which any use, modification or distribution must be put to the author's approval.

3. The relevance of French intellectual property law regarding blockchain components

The tenets of French intellectual property law apply to the components of blockchain as defined in this article and particularly copyright rules. We must tackle the issue of patent law as well as the uncertainties regarding the protection of some blockchain components.

3.1. Software, visual interfaces and copyright protection

Standard copyright rules for visual interfaces

The blockchain is composed, amongst others, of software programs and visual interfaces. Pursuant to article L.111-1 of the French Intellectual Property code, "the author or a work of the mind shall enjoy in that work, by the mere fact of its creation, an exclusive incorporeal property right which shall be enforceable against all persons." Accordingly, article L. 112-2 of this code provides a non-exhaustive list of the works that can be protected by copyright law, which protects all "creator" of original work against the operation by any third party.

[85] *Ch. Caron, Les licences de logiciels dits "libres" à l'épreuve du droit d'auteur français : D. 2003, p. 1556*
[86] *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, SEC, July 25, 2017*

Specific provisions governing software programs

A software program written in a different markup language from previous software must be construed as original work if this new language enables said software to be run on certain types of processors; this improvement meets the requirement of "*the existence of a specific intellectual input and personal effort*". Therefore, the blockchain, which is made of software programs such as smart contracts, will be protected and its authors and programmers can monitor and even prevent their computer program from being used, provided they prove said *"existence of a specific intellectual input and personal effort"*.

Given the technical specificities of software programs, the rights granted to the author of such work of the mind are governed by specific provisions. For instance, the author of a software program may forbid "*the permanent or temporary reproduction of software by any means and in any form*". This author may also prevent *"the translation, adaptation, arrangement or any other alteration of software and the reproduction of the results thereof."*[87]

Sharing the rights: the practical implementation of the provisions for components created by more than one person

French law provides different protection standards according to the participation in the creation of the software.

Collaborative work ensures equal rights to its creators. In practice, a software program constitutes collaborative work when its authors have consulted each other, worked towards a same goal on an acceptably equal footing[88].

Composite or derivative work grants rights to the consecutive software creators. These include, for instance, a part of a preexisting source code incorporated into a new software program. The creator of the new, original work will own the rights but will have to comply with that of the creator of the previous creation.

For public blockchains, the trend is to develop free sublicenses which create fewer legal constraints for new developments, although it all depends on the license the author chose.

Data ownership

Who does the data - i.e. the history of all the blockchain transactions - belong to? Databases, defined in article L. 112 of the French Intellectual Property code as *"a collection of independent works, data or other materials, arranged systematically or methodically and that can be accessed by electronic or any other means"* allow their authors to prevent the database they created from being extracted or reused. Databases integrated to a blockchain could therefore belong to the people who initiated the storage of data in blocks. The data would, however, belong to the person this information pertains to. This is true for so-called "private" data, that may directly or indirectly identify a natural person. This data "falls under a fundamental, non-transferable right, the right to privacy"[89].

3.2. The possibility of software protection by patent law

In France, *"New inventions which involve an inventive step and are susceptible of industrial application, are patentable."*[90].

Consequently, the National Institute of Intellectual Property (INPI) states that "should a computer program, run on a computer, be able to produce an additional technical activity to the normal technical activity of running the computer in question, the software may be patentable."

Therefore, in France, by patent law may protect blockchain software programs that meet the previous requirements. In the US, the USPTO, The US Patent and Trademark Office counted 71 patents relative to blockchain and cryptocurrency technology in 2012. In 2016, the number could be as high as 469 patents[91].

3.3. The uncertain protection of algorithms and the applicability business secrecy

Some blockchain components cannot be protected by copyright, or patent right. For instance, algorithms, for which the INPI uses the Larousse dictionary definition, i.e. *"a set operative rules whose implementation would solve a problem set out as a fix number of operations. An algorithm may be translated, by means of a markup language, into a program that can be run by a computer."*[92]

[87] *Article L.122-6 of the French Intellectual Property code*
[88] *CA Paris, pôle 5, 1re ch, 27 févr. 2013, n)11/11785 : Propr. Intell.2013, n) 47, p.188, obs. A. Lucas.*
[89] *"A qui appartient nos données ?"- 26 novembre 2014 : http://www.cil.cnrs.fr/CIL/spip.php?article2611*
[90] *Article L.611-10 al. 1 of the French Intellectual Property code*
[91] *https://cointelegraph.com/news/blockchain-patent-applications-almost-double-in-q1-2017-uspto-data*
[92] *"La propriété intellectuelle et la transformation numérique de l'économie" - Marc Schuler et Benjamin Znaty - https://www.inpi.fr/sites/default/files/1_3_extrait_pi_et_transformation_economie_numerique_inpi.pdf*

Therefore, in and of themselves, algorithms - because they are mathematical principles - are ideas and must therefore "flow freely" unhampered by patents.

In conclusion, from a practical point of view, the difference between public and private blockchains could have an impact on intellectual property rights: only the creators of private blockchains may be protected as they have kept their algorithms secret.

C. BLOCKCHAIN AND THE PROTECTION OF PERSONAL DATA

A blockchain being defined as a register of transactions that is tamper-proof, distributed, verifiable by all and based on a consensus, it follows that the transactions recorded in a blockchain are intended to be unalterable and therefore non-removable. Although it is possible to cancel a transaction by means of an opposite transaction, it is not possible to delete a transaction.

However, the GDPR[93] provides for a right to erasure[94]. It is therefore legitimate to question the compatibility of the definition of blockchain with this Regulation.

1. Personal data, anonymized data and pseudonymised data

The GDPR applies to the processing of personal data, which is defined broadly as any information relating to an identified or identifiable natural person, including by reference to an identifier, or to one or more specific elements pertaining to his identity. On the other hand, when the data is anonymous or anonymised, i.e. when the data does not allow the person concerned to be directly or indirectly re-identified, the GDPR does not apply.

The GDPR mentions a third category of data, pseudonymous data[95], i.e. data which is non-nominative but which nevertheless allow the indirect identification of an individual and is therefore considered as personal data subject to the rules of the GDPR.

The blockchain generally uses non-nominative identifiers, the purpose of which is to be able to re-identify the participants in a transaction without publicising the personal data concerning them.

Even though some commentators mention that blockchains that deal with transactions between individuals are "anonymous", it is pseudonymous data, i.e. personal data that is subject to the GDPR rules.

2. The right to erasure according to the GDPR

According to the GDPR, the right to erasure is the right of an individual to request that his personal data be erased, especially when the following conditions are met:

- the personal data is no longer necessary for the purpose for which it was collected;
- the data subject withdraws his consent to the processing and it cannot be based on any other legal basis; or
- the data subject objects to the processing without there being a compelling legitimate reason for the processing.

Moreover, even though the GDPR provides exceptions to the exercise of the right to erasure, for example when the processing is necessary for archival purposes in the public interest or for statistical purposes, these exceptions do not appear to us to be applicable to transactions between individuals registered in a blockchain.

If the definition of the blockchain seems incompatible with the right to erasure, are there solutions to remedy this situation? In the absence of an amendment to the GDPR, two approaches can be envisaged.

Firstly, it seems to us that when a person concerned is clearly and previously informed that in the event of participation in a blockchain, the conditions for exercising his right to erasure are

[93] *Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The GDPR being applicable from May 25, 2018 and replacing French law no. 78-17 of January 6, 1978 relating to computers, files and freedoms, we will not detail the differences that may exist with the right to erasure as provided for by this law.*

[94] *See Article 17 of the GDPR, entitled "Right to erasure ("right to be forgotten"). Although the term "right to be forgotten" is often used, we will use "right to erasure", since it appears more precise.*

[95] *According to the GDPR, pseudonymisation is "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".*

rendered inapplicable, and this waiver is accepted, this right to erasure may become legally unavailable. It would be possible to inform the person concerned that:

- the very purpose of a blockchain is the retention of the data of the transactions it contains in an unalterable way over time, and that consequently, the data will always be necessary with regard to the purposes for which it was collected;
- beyond the transaction that he carries out, his consent relates to the inalterable retention of his data in the blockchain, necessary for his transaction, and that in all cases, the legitimate interest of the data controller could justify this processing;
- despite his opposition to the processing, the reliability of the blockchain over time is a compelling legitimate reason for this data not to be erased.

On the other hand, notwithstanding the above definition, a blockchain can be modified by the consensus of its community, especially to correct or change it, as demonstrated by the recent split of Bitcoin in 2017 or that of The DAO in 2016. The communities could therefore decide to organise, in limited and well-defined cases, procedures allowing the exercise of the right to erasure, in one form or another. Indeed, the objective of the right to erasure (or right to be forgotten) is to make personal data inaccessible; a result that can be obtained by erasure, but also for example by irreversible anonymization. Since it is no longer possible to directly or indirectly identify an individual through the transaction in which he participated, the objective of the right to erasure is achieved. So if it is not possible to delete a transaction, it is probably possible to conceal the personal data of this transaction or to make it inaccessible, irreversibly.

Subject to the technical feasibility of such an anonymisation solution, each of these two approaches could make it possible to reconcile the operation of blockchain with the imperatives of the protection of personal data.

D. BLOCKCHAIN AND ELECTRONIC SIGNATURE

The blockchain is, as seen previously, a ledger of shared data in a network composed of blocks that guarantees the anonymity of transactions and was created in order to remove intermediaries (in the case of Bitcoin's blockchain: banks). As for electronic signature, it is a process that aims to ensure the identification of a signatory, which is, in most cases, guaranteed by the intervention of a trustworthy third party.

The blockchain and the electronic signature thus seem quite incompatible. However, they are both based on the same underlying technic: asymmetric cryptography (1).

Henceforth, one may wonder about the possibility of using blockchain technology in order to develop an electronic signature solution which would meet the security and trust requirements of French and European regulations (2).

Such a solution could compensate some flaws of conventional electronic signature solutions (3). Nevertheless, new difficulties could also arise from this solution (4).

1. Asymetric cryptography

Both blockchain and electronic signature are based on mathematical discoveries from the last century, in particular encryption.

These discoveries have made possible the elaboration of a new encryption technique based on two keys.

With traditional encryption (symmetric encryption), the message was encrypted and decrypted using only one key. This technique presented great difficulties: transmission of the code had to be secured and the encryption was made more vulnerable every time the range of people having knowledge of the code grew wider.

In order to overcome these difficulties, asymmetric encryption has been developed. This encryption method is based on the use of two distinct encryption and decryption keys: a private key (which is only known to its holder) and a public key (which can be known to everyone). The public key is calculated in a unique manner from the private key. Only the private key is able to decrypt an encrypt message using the public key on which the message is associated. This duplication limits the transfer of a secret key: if a person A wants to transmit a confidential message to B, he can encrypt such message with the public key of B (which can be freely transmitted) and B will be the only one having the ability to decrypt this message with his public key.

The reverse is also true: only the public key combined with the private key can decrypt a message which has been encrypted by the private key.

Therefore, this method is of particular interest for authentifying people: since only the holder knows his private key, encrypting a message using this private key enables to ensure that the message has been sent by the holder itself.

The electronic signature is therefore based on this asymmetric encryption method. Firstly, the signatory will create a "hash" of his message (i.e. a cryptographic digest presented as a sequence of fixed-length alphanumeric characters representing the message content, without revealing it, and the unique value of which is generated by a hash algorithm). Then, the signatory will use his private key to sign his message. Any modification of the message would then render the signature invalid because the hash would no longer match the message.

Afterwards, the recipient can decrypt the hash using the sender's public key. If both keys match, the recipient can be relatively confident about the identity of the sender and the origin of the message.

The blockchain also works by means of this asymmetric cryptology method. When using the blockchain for the first time, the user will be allocated a public and private key pair. Its blockchain "address" will be calculated from his public key. When the user wishes to carry out a transaction on the blockchain, he will encrypt the hash of his message with his private key. Then, the miners verify that the private key matches the public key stored in the blockchain in order to validate the transaction (when it is about a transaction involving cryptographic currency, the miners will ensure that the sender has the necessary funds for the transaction).

2. Blockchain and eIDAS regulation

Since the blockchain is, as described by its creator Satoshi Nakamoto[96], "a chain of electronic signatures", we could imagine creating a blockchain that is an electronic signature solution for documents and agreements.

The difficulty will then be to comply with the provisions of the Regulation on electronic identification and trust services for electronic transactions in the internal market[97] (hereinafter "eIDAS Regulation"), which regulates, among other things, electronic signatures.

The eIDAS Regulation identifies three types of electronic signatures, which correspond to the three types of signatures identified by the 1999 Directive and the 2001 French Decree[98].

The three signature levels are: simple, advanced (the secured signature in France) and qualified (the presumed reliable signature in France).

Article 25 of the eIDAS Regulation lays down the principle of non-discrimination between electronic signatures regarding the burden of proof. Under this section, all electronic signatures must be accepted as evidence. However, it is up to the person claiming it to prove their reliability. The burden of proof can be reversed only by the using of a qualified signature and thus benefiting from a presumption of reliability.

Given the probationary risks posed by the simple and advanced electronic signature, we will try to assess if an electronic signature solution based on the blockchain could meet the (very strict) requirements of qualified signatures.

2.1. Simple signature

At this time, there is no particular regulatory framework regarding the simple signature.

Any acceptance of an online contract (e.g. by simply ticking a box to accept the terms and conditions of sale) is a simple electronic signature.

As a consequence, this kind of signature could be easily implemented in a blockchain since it is already what it is used presently to carry out transactions.

However, this kind of signature contains a strong risk regarding the burden of proof since it will be uneasy to identify the signatory and demonstrate the reliability of the electronic signature process.

2.2. Advanced signature

Four cumulative conditions must be met regarding the advanced signature.

Firstly, the signature must be unambiguously linked to the signatory. Then, such signature must provide the identification of the signatory. In addition,

[96] *Satoshi Nakamoto, Bitcoin: a Peer-to-Peer Electronic Cash System, 31st October 2008.*
[97] *Regulation (EU) No 910/2014: of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ("eIDAS")*
[98] *Decree No. 2001-272 of 30 March 2001 implementing article 1316-4 of the Civil Code relating to electronic signatures.*

the signature must be created with creation's data of the electronic signature that the signatory can, with a high level of confidence, use under its exclusive control. Finally, the signature must be linked to the data connected with that signature in such a way that any subsequent changes to the data be detectable.

The first three conditions of the advanced signature are related to the creation, storage and use of the public/private key pair issued to the signatory.

With regard to the first condition, the principle of asymmetric cryptography will enable, through its public key, to identify the private key holder. Since the public key matches in a unique manner with the private key, and the private key is a secret key, the key pair checks that the signature unambiguously matches with the signatory.

The second condition refers to the necessity to link the public and private key pair to the particular person's identity, so that it can be ensured that it is an identified individual who uses the key pair in question. In general, this condition is met by the concomitant issuance of (i) a certificate indicating the identity of the person and his public key and (ii) the key pair. The certificate is issued after verification of the signatory's identity. This verification can be implemented in several ways, which can be more or less restrictive: sending identity documents, verification by sending a code by SMS or e-mail, face-to-face appointments, etc. The more stringent the method of verification of identity is, the easier it will be to bring the proof of the certificate's reliability.

The third condition is to demonstrate that the signatory is the sole master of his private key, which cannot be used by anyone else and cannot be counterfeit. However, at this time, no definitive standard has been adopted to specify (i) what constitutes a "high level of confidence of sole control" and (ii) what means are granted to identify signatories. In this respect, the ANSSI has published a document setting forth that "the means implemented must ensure an adequate level of security and mitigate the risk of fraud upon signature[99]". The ANSSI gives, as an example, the use of a PIN code provided for this purpose, which would enable the signatory to unblock the use of his private key, which may be contained on his terminal (computers, mobile phones, etc.).

The last condition is usually met by performing a "hash" of the message before signing it electronically, this ensures the signed message integrity over time, as detailed above.

This second type of signature provides evidence which, in case of dispute, could provide the proof of the signature, its reliability and the identity of the signatory. This intermediate solution is often the preferred one for companies. However, the various actors involved in electronic signatures (certification authorities, software publishers, etc.) prefer using, in practice, standards published by European committees regarding qualified signatures, even for advanced signatures[100].

These standards include the issuance of a certificate after a physical meeting with the certification authority or a third party, as well as the certificate's supply on a hardware cryptographic support (USB key...). This would make the adoption of an advanced level of electronic signature much more binding without reversing the burden of proof.

Regarding its implementation in the blockchain, it will be necessary to ensure that all key pairs used within the blockchain are delivered using the same protocol, so that a private key cannot match with two public keys issued by two different operators using different protocols.

In addition, the allocation's requirements for key pairs and certificates should be strengthened in order to meet the requirements provided above. Operators should be able to verify the person's identity, and the key pair as well as the certificate should be transmitted securely and linked with a PIN code known only by the signatory.

2.3. Qualified signature

Regarding the qualified signature, three cumulative requirements must be met.

Firstly, the signature must be an advanced electronic signature (and thus fulfil all the criteria provided above). Then, the signature must be generated using a qualified electronic signature creation device (Article 29 and Appendix II). Finally, this device must be based on a qualified certificate of electronic signature (Article 28 and Appendix I) delivered by a trustworthy service provider (i.e. an accredited provider by a national entity), which must, in particular, verify the person's identity by using a face-to-face check (Article 27 (1)(a)).

This kind of signature would require a trustworthy service provider to develop an electronic signature

[99] *ANSSI, Regulation eIDAS – FAQs, 2nd June 2016*

[100] *In particular the CEN (European Committee for Standardization) and ETSI (European Telecommunications Standards Institute) standards with the ETSI EN 319 411 - 1 standard.*

protocol operating on the blockchain. Furthermore, this protocol must comply with all technical standards laid down by the European Commission.

3. Practical value of such solution

The traditional solution of the electronic solution can present several technical and organizational issues that could be avoided by using a blockchain solution.

Firstly, an electronic signature solution requires the intervention of several actors: the third-party certifier, the time stamping provider, the archiving provider and the signature software supplier. This increases the chance of errors and technical difficulties while diluting liability towards the customer.

A blockchain electronic signature solution could potentially require the use of far fewer actors since each block is time-stamped and also provide the storage of the signed document. Nevertheless, if the signature implemented is a qualified signature, the use of a third party certifier remains mandatory.

Moreover, the price per signature offered by traditional operators is relatively high and must be added to the costs involved in archiving documents. Blockchain transactions could be offered for a small fee.

Finally, the electronic signature solution would be much more secured on the blockchain.

Therefore, the blockchain solution for electronic signatures seems to be an advanced solution much more pragmatic, efficient, economical and secure.

4. Issues regarding the use of blockchain as an electronic signature solution

In addition to the eIDAS compliance difficulties mentioned above, a blockchain electronic signature solution seems to present two major difficulties which, in our view, could be resolved.

These two difficulties are due to the public nature of the blockchain network and the information it contains. This could frighten contractors/signatories who wish to (i) keep the terms of their commitment confidential and (ii) make their identity and the person with whom they contract inaccessible to anyone.

The first difficulty is easily avoided by integrating only a "hash" of the contract and not the entire agreement into the block signed by the parties. This solution also has the advantage of reducing the weight of the block and requires less storage space.

The matter of confidentiality of the signatories then arises. This is a particularly sensitive issue, since the whole point of an electronic signature solution is precisely to make the verification of the signatories' identity possible. Therefore, it will be necessary to elaborate a signature which enables all signatories to be identified by each other but also to conceal their identity from any third party to the transaction.

However, the use of asymmetric cryptology as described above could enable anyone with the signatory's public key to have access to all contracts signed by the signatory.

Nevertheless, this problem could be avoided by the use of multiple signatures or ring signatures which enable to link public keys of different signatories in order to create a new public key unique to the transaction.

Multiple signatures are already supported by some blockchains but should be improved to provide the transaction validation only when all signatories have signed the block.

This highly technical point of contention should be the object of further developments.

E. BLOCKCHAIN AND CYBERSECURITY

Blockchain & Cybersecurity are two key notions in the digital world. Cybersecurity has been defined by the French National Cybersecurity Agency ("ANSSI") as a desired state for an information system allowing it to withstand events from cyberspace that could compromise the availability, integrity or confidentiality of data stored, processed or transmitted and the services that such systems offer or make available.

However, nowadays cybersecurity is a major issue, with the number of cyberattacks increasing. In the financial sector, the most exposed platforms are the digital platforms where various crypto-currencies are traded.

Today in France, cyber criminality is subject to the provisions of the Criminal Law Code – applicable

to attacks targeting IT systems as well as attacks using IT systems. The financial sector is currently organising new regulations in order to establish liabilities between the operators.

1. Legal protection applicable to attacks targeting IT systems

In the financial sector, where confidentiality is of the essence, the security of blockchains is a major concern amongst the companies envisaging implementing this digital tool.

French criminal laws have established protection against attacks targeting "automatized data processing systems"[101] **("ADPS")**, the definition of which encompasses any IT software, system or device protected by security mechanisms. It can be assumed that blockchain would fall within the scope of this definition.

French provisions on ADPS[102] incriminate any intrusion into IT systems, as well as actions performed so as to hinder a system's functioning, or the modification or suppression of data. These types of misconduct also fall under the scope of French criminal laws when performed by a criminal association.

Other provisions which could apply would be those concerning the provision of equipment, instruments or software, which have been elaborated or adapted in order to commit offences targeting ADPS. It can be assumed that these provisions could have been applied in a case such as the DAO[103] attack in June 2016 which was performed thanks to a loophole in a "smart contract".

2. Legal protection applicable to attacks using networks

Attacks using the Web can fall within the scope of various offences.

For example, extortion[104] has already been held against individuals who have blocked company IT systems in an attempt to obtain commercial advantages over the company. This kind of behaviour could possibly target data stored in a blockchain. Alternatively, DDoS[105] attacks could be organised to obtain wire transfers or transfers of financial securities in return. It should be highlighted however, that such attacks are in fact very difficult to implement considering the decentralised organisation of a blockchain.

It could also be envisaged that data might simply be stolen from a blockchain – however, case law has recognised the existence of theft even when committed in the digital world[106].

3. Liabilities of operators in the financial sector with regards cybersecurity

Previously cybersecurity in the financial sector has been a mere concept, embedded in the mass of obligations applicable to financial companies aimed at ensuring the allocation of sufficient human and material (including IT) resources to financial activities.

But, following the transposition of Directive 2015/2366 of 25 November 2015, cyber-attack finally appears among the types of "security incident" which should be notified without delay to the Banque de France from 13 January 2018.

This obligation seems to be only applicable to payment service providers at this stage – however, it is possible that the scope of this obligation could be extended by the French Prudential Control and Resolution Authority ("ACPR").

As a conclusion, French laws are sufficiently comprehensive and consistent to apprehend attacks which could target a blockchain or use its functionalities. However, with technology generally evolving at lightning speed, the law will certainly have to adapt accordingly.

[101] *Report elaborated by the French Senate, 22 December 1987, see page 13.*
[102] *Articles 323-1 to 323-8 of the French Criminal Code.*
[103] *Decentralized Autonomous Organization related to Ethereum.*
[104] *Article 312-1 of the French Criminal Code.*
[105] *Distributed Denial of Service.*
[106] *French Supreme Court, 20 May 2015, Nr 14-81336.*

F. GOVERNANCE OF A BLOCKCHAIN IN POST-TRADE ACTIVITIES

The governance of a distributed and decentralized network like that of blockchain is at the heart of the power and financial stakes. However, there is no governance of blockchain, but as many modes of governance as there are types of distributed networks. In fact, the mode of operation of a distributed network determines its governance.

The *Proof of Work and the Proof of Stake* are the two ways to validate the most well-known blocks. They involve two very different consensus mechanisms, described in greater detail above.

It is impossible in a distributed computing system to guarantee at the same time (i.e. synchronously) the three following constraints:

- consistency: all nodes in the system see exactly the same data at the same time;
- availability: guarantee that all requests are responded to; and
- partitioning tolerance: no failure less severe than a total network outage should prevent the system from responding correctly.

Any distributed computing system can only guarantee at a time *t* compliance with two of these constraints, but not all three. This is the challenge that must be met by the mode of governance. This is different depending on whether public, semi-public or private channels are concerned.

The main advantage of the blockchain being the security of transactions, its governance depends on its mode of operation.

To avoid being falsifiable, a blockchain using a proof of work consensus method requires that no hostile operator holds, at any time, more than half the computing power of the chain.

In public blockchains, governance is in the hands of miners, i.e. those who validate transactions. The users *(stockholders)* have little or no voice in the chapter. An illustration of this can be found in the *fork* of Bitcoin during the summer of 2017. Finally, it was the miners who decided to adopt an amendment to the protocol.

It is clear that in blockchains on the financial markets, the regulator will have a leading role to play in monitoring the non-falsifiability of consensus chains.

Another governance issue stems from the compatibility between anti-money laundering standards and the structure of the block where transactions are recorded under a pseudonym, through public keys, in addition to private keys.

In the field of post-trading activities, the issue of governance is just as important. In fact, it is a matter of determining whether the operation of decentralized and distributed registers can be entrusted to third-party individuals or entities, not to mention the fact that in the case of public blockchains, miners are located outside Europe (in practice in Asia and especially in China) which necessarily raises a question of sovereignty.

Of course, if the blockchain technology used in the post-trade activities is a private channel, therefore closed, the governance will then approach that of a consortium, or even simply of a public limited company, i.e. a sharing of power between the owners of the technology.

G. CONFLICTS OF LAW IN POST-TRADE ACTIVITIES

Insofar as a court will sooner or later have to rule on a dispute concerning a DLT, the question of determining the jurisdiction of this court under the rules of private international law arises.

The question becomes even more specific in the area of financial securities where various texts establish or clarify the rules of jurisdiction in matters of conflict of laws.

At the international level, the Hague Convention of July 5, 2006 on the law applicable to certain rights on securities held with an intermediary, although ratified by a very limited number of countries, constitutes an important reference in the criteria for determining the law applicable to securities.

Within the European Union, there are various harmonised conflict of law rules that apply to financial securities:

- The Settlement Finality Directive in respect of account securities provided as collateral to participants in settlement systems, of the ECB or the central bank of the Member States;
- Directive on the collateralisation of book-entry securities within the framework of financial contracts;

- Liquidation Directive concerning the enforcement of proprietary rights on book-entry securities in the insolvency proceedings of credit institutions and investment companies.

In these texts, the three conflict of laws rules are based on a similar approach: the PRIMA concept, as used in the Hague Convention, i.e. the location of the relevant intermediary.

The connecting factors in the three European Directives differ in detail, but can be summarised as follows: it is a register, an account or a centralised deposit system. However, the concepts of "register" or "account" are not defined or are poorly defined in these texts. In fact, these conflict of law rules do not specify where the account / register, centralised deposit system is "located" or "maintained".

The PRIMA rule departs from traditional connecting factors referring to the place of incorporation of the issuing company. Instead, this rule refers to the law of the securities account to which the securities concerned are credited. This law governs all securities credited to this account, whether foreign or domestic.

What could be the connecting factor to consider the nature of the law as well as the conditions of acquisition and disposal in a blockchain system?

The PRIMA rule presupposes the existence of accounts and therefore intermediaries, which will not exist as such in the implementation of the block. It is therefore necessary to exclude this conflict of law rule, which is not suited to the case of a distributed and decentralised register.

First possible connecting factor, the law of the issuer of the securities, or lex societatis. This criterion, which would certainly create significant legal uncertainty because of the multiplicity of potentially applicable laws in the case of an international portfolio seems, however, the most appropriate because of the unsuitability of the two criteria detailed below.

Second possible connecting factor, the entry point of the blockchain. This factor, however, does not solve the problem as there are as many entry points as there are participants in the chain.

Third possible connecting factor, the law of the jurisdiction where the system is located or supervised. It is still necessary that the register of blocks or the administrator of this register is regulated, which is not possible in a public blockchain.

In fact, in terms of post-trade activities, and since the operation of the blockchain will instead involve a private or semi-private blockchain, the solution could be to impose on the managing administrator the distributed register to be approved by the supervisor of the place where it is incorporated in respect of a new activity, namely that of holder of a distributed register.

H. RESPONSE TO THE CONSULTATION OF THE TREASURY

As mentioned in the introduction, this report is a general response to the Treasury Department's consultation aimed at informing public authorities to help them develop the legislative and regulatory framework applicable to distributed registers.

The objective of the working group is to make proposals or recommendations to the public authorities to allow the use of DLT in post-trade activities. This includes using the opportunities provided by the Sapin II Law to legislate by way of decree.

The following proposals are limited to legislative provisions and do not deal with regulatory changes.

CONTRIBUTORS TO THE PARIS EUROPLACE BLOCKCHAIN COMMITTEE

CHAIRMAN:

Hubert de Vauplane, Partner, Kramer Levin Naftalis & Frankel LLP

MEMBERS:

Emilien Bernard-Alzias, Partner, Simmons & Simmons LLP

Céline Bondard, Partner, Bondard et ass.

Alexis Collomb, Professor at the CNAM

Emilie Danglades-Perez, Partner, Simmons & Simmons LLP

Carine Delfrayssi, Director, Paris Europlace

Thierry Dor, Partner, Gide Loyrette Nouel AARPI

Jean-Gabriel Flandrois, Partner, Gide Loyrette Nouel AARPI

Alexandre Léger, Founder and CEO, eCapitalio

Alain Pithon, Secretary General, Paris Europlace

Eric Roturier, Partner, Allen & Overy LLP

Guillaume Seligmann, Partner, Cohen Gresser

AFTI

AFG

Euroclear

BNPP Securities Services

GLOSSARY

The financial, economic or computer science vocabulary is the subject of ad hoc opinions from the Commission for Enrichment of the French Language published in the Official Journal. The opinion of the Commission published in the Official Journal of May 23, 2017 (NOR: CTNR1713838K) on computer science vocabulary defines the main terms relating to blockchain. Terms and definitions adopted by the Commission are marked with an asterisk (*).

English term	French term	Definition
Block validation	Validation de bloc*	Computer operation used to make a block tamper-proof and validate it in a blockchain.
Consensus	Consensus	Mechanism to ensure that each network node has the same information before permanently recording a transaction in the blockchain.
Cryptocurrency	Crypto-monnaie ou Cybermonnaie*	Currency whose creation and management are based on the use of IT and telecommunications techniques. *
Distributed ledger technology	Registre partagé distribué	Data registry shared between all participants in the blockchain. Only the validation of a transaction through a consensus can modify its content.
Fiat money	Monnaie légale	Term designating State currencies which are legal tender and with discharging power. In particular, they oppose cryptocurrencies, which have no legal value of their own.
Fintech	Entreprises de technologie financières	This term, a contraction of "technology" and "finance", refers depending on the context to new technology companies specialising in the design of innovative services in the field of finance, or the services themselves.
Miner	Mineur	Natural or legal person providing its computing power for the purposes of mining.
Mining	Minage*	Block validation giving rise to the creation of new units of account for the benefit of the participant whose block has been retained by the network.*

English term	French term	Definition
Node	Nœud	Hardware connected to the blockchain that is responsible for performing the calculations. (see also "miners").
Peer-to-peer	Pair à pair*	The mode of use of a network in which each of the connected participants has the same rights and which allows a direct exchange of services without resorting to a central server; by extension, the term is used to describe such a network.*
Private blockchain	Chaîne de blocs* privée (ou "fermée")	Type of blockchain whose access is reserved for certain participants.
Private key	Clef privée	The private key is used to decode a message previously encrypted by the public key. Unlike the public key, the private key is known by a single user.
Proof of Concept ("PoC")	Preuve de concept	Demonstration of the feasibility of a concept by means of a short presentation drawn from a concrete case.
Proof of Work ("PoW")	Preuve de travail*	The result of a task that consumes a lot of computing resources, the accuracy of which is easily verifiable by any participant and attests that this task has been carried out by consuming the necessary resources. Proof of work is used in particular to contribute to the establishment of user confidence in a cybercurrency, fraud being discouraged by the difficulty of block validation.*
Public blockchain	Chaîne de blocs* publique (ou "ouverte")	Type of blockchain whose access is open to any participant who wishes to intervene.
Public key	Clef publique	Known to all, the public key is the address of the blockchain. It allows to encode a message and will be used so that an issuer can designate a recipient within the framework of a transaction.
Smart contracts	Contrats intelligents	Digital contracts which make it possible to execute their terms without human intervention.
Token	Jeton	The token is a basic unit that can be transmitted within a distributed register (e.g. the token of the Bitcoin chain is Bitcoin). The token can also contain information beyond their quasi-monetary aspect (information on ownership, the direction of a vote, or any other information).

ANNEXE 2

BIBLIOGRAPHY

- A. Santo et al. "Applicability of the Ditributed Ledger Technology to Capital Market Infrastructure", Japan Exchange Group, Working Paper, 3O August 2016, vol. 15.

- A. Benssoussan, Le robot créateur peut-il être protégé par le droit d'auteur, Planète Robot n°42, accessible à l'adresse suivante : https://www.alain-bensoussan.com/wp-content/uploads/2016/12/34125221.pdf.

- BRI, Central bank cryptocurrencies, septembre 2017, accessible à l'adresse suivante : https://www.bis.org/publ/qtrpdf/r_qt1709f.htm.

- C. Caron, Les licences de logiciels dits "libres" à l'épreuve du droit d'auteur français, D. 2003, p. 1556.

- M. Dantant, Droit d'auteur des chercheurs, Logiciels, Bases de Données et Archives Ouvertes, CNRS, Direction des affaires juridiques, 7 juillet 2014.

- W. Diffie et M.E. Hellman, New Directions in Cryptography, 6 novembre 1976.

- ECB, Distributed Ledger Technolgies in securities post trading, revolution or evolution, Occasional paper series, n° 172, April 2016.

- Euroclear and Oliver Wyman Joint Report, "Blockchain in the Capital Markets – The Prize and the Journey", February 2016.

- Euroclear and Slaugther & May Joint Report, "Blockchain Settlement: Regulation, innovation and application", November 2016.

- P. de Filipi et B. Jean, Les smarts contracts, les nouveaux contrats augmentés ? La revue de l'ACE, septembre 2016, n°137.

- D. Galeon et P. Caughill, Major Players Unite to Define Blockchain Token Securities Law, 7 décembre 2016, accessible à l'adresse suivante : https://futurism.com/major-players-unite-to-define-blockchain-token-securities-law.

- IMF Staff Discussion Note, Virtual Currencies and Beyond: Initial Considerations, janvier 2016.

- IMF Staff Discussion Note, Fintech and Financial Services: Initial Considerations, juin 2017, accessible à l'adresse suivante : http://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2017/06/16/Fintech-and-Financial-Services-Initial-Considerations-44985.

- ISDA Whitepaper, The Future of Derivatives Processing and Market Infrastructure, septembre 2016.

- ISDA / Linklaters Whitepaper, Smart Contracts and Distributed Ledger – A Legal Perspective, août 2017.

- M. Jacob, Panorama de la cybercriminalité du CLUSIF : l'industrie du malware ne connait pas la crise! Global Security Mag, janvier 2017.

- Kramer Levin, Gestion du passif des OPC et enjeux réglementaires, juillet 2014.

- L. Lamport, R. Shostak et M. Pease, The Byzantine Generals Problem, 5 juillet 1982.

- L. Lessig, Code is Law, Harvard Magazine, janvier 2016, accessible à l'adresse suivante : http://harvardmagazine.com/2000/01/code-is-law-html.

- M. Mainelli et A. Milne, The impact and potential of blockchain on securities transaction lifecycle, 9 mai 2016, accessible à l'adresse suivante : http://www.swiftinstitute.org/wp-content/uploads/2016/05/The-Impact-and-Potential-of-Blockchain-on-the-Securities-Transaction-Lifecycle_Mainelli-and-Milne-FINAL.pdf.

- S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 31 octobre 2008, accessible à l'adresse suivante : https://bitcoin.org/bitcoin.pdf.

- P. Paech, "Securities, intermediation and the blockchain - an inevitable choice between liquidity and legal certainty?" Uniform Law Review (2016) 21 (4) pp.612-639.

- P. Paech, "'Securities, intermediation and the blockchain - an inevitable choice between liquidity and legal certainty?" LSE Law and Economy Working Paper Series 20/20150.

- R.L. Rivest, A. Shamir, and L. Adleman A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, février 1978.

- M. Schuler et B. Znaty, La propriété intellectuelle et la transformation numérique de l'économie, accessible à l'adresse suivante: https://www.inpi.fr/sites/default/files/1_3_extrait_pi_et_transformation_economie_numerique_inpi.pdf.

- H. de Vauplane, La Blockchain et la loi, La finance décryptée par le Droit, 14 février 2016.

- A. Wright and P. De Filippi, "Decentralised Blockchain Technology and the Rise of Lex Cryptographica" (2015) Working paper, 11-12, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.

- P. Yolka, Prendre les "communs" au sérieux, AJDA 2016. 1.

PARIS EUROPLACE

About Paris EUROPLACE:

Paris EUROPLACE is the organisation in charge of developing and promoting the Paris Financial Marketplace and the French financial industry internationally. It brings together all financial industry stakeholders; its 400+ members include issuers, investors, banks and financial intermediaries, insurance companies, attorneys and accountants, consulting firms, etc. The association is chaired by Gérard Mestrallet, Chairman of the Board of ENGIE.

www.paris-europlace.com

Paris EUROPLACE

@europlace