

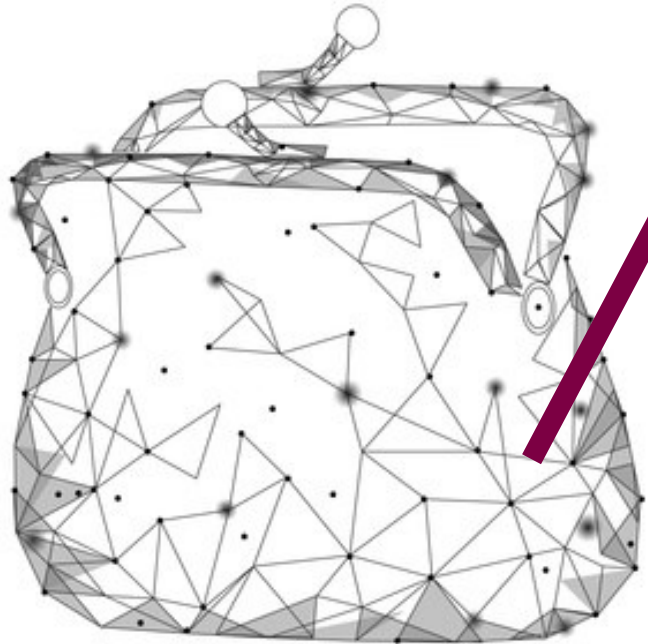
January 2018



Blockchain

8 main legal issues

- What is the Blockchain ?
- Can it be regulated ?
- In which spheres does it come into play ?
- What about the protection of personal data (GDPR) ?



This document is the property of the law firm Mathias Avocats. Any reproduction and/or representation is subject to the prior consent of the firm Mathias Avocats and to provisions of the French Intellectual Property Code.

SOMMAIRE

INTRODUCTION	04
WHAT IS THE BLOCKCHAIN AND ARE ITS LEGAL IMPLICATIONS ?	05
WHAT ARE SMART CONTRACTS ?	07
HOW CAN BLOCKCHAIN PROTECT INTELLECTUAL PROPERTY RIGHTS ?	09
HOW CAN BLOCKCHAIN AND TRADE SECRETS SUPPORT EACH OTHER ?	11
WHO IS LIABLE FOR THE BLOCKCHAIN ?	13
WHAT IS AN INITIAL COIN OFFERING (ICO) ?	16
BLOCKCHAIN AND THE GDPR : HOW DO THEY INTERACT ?	18
NEW REGULATIONS FOR THE BLOCKCHAIN ?	21

INTRODUCTION

La « blockchain » ou en français une chaîne de blocs est et reste une technologie de stockage et de transmission d'informations. En quelques mots, cette chaîne de blocs, publique ou privée, est avant tout une base de données (registre de toutes les opérations).

Toutefois, le caractère décentralisé de cette technologie fait qu'elle n'obéit ni à une gouvernance, ni à une régulation dédiée. Ainsi, cette chaîne de blocs peut être utilisée pour protéger des créations ou être le véhicule d'instruments financiers : c'est un nouveau vecteur de confiance.

Afin de favoriser cette confiance, la prise en compte des aspects juridiques est essentielle notamment en termes de contrats, de propriété intellectuelle, de responsabilité ou encore de conformité (RGPD).

En tant que Conseil, nous sommes confrontés quotidiennement à la gestion des enjeux stratégiques, nous accompagnons les acteurs dans leur innovation et leur conformité.

Nous vous souhaitons une bonne lecture, en espérant sincèrement que cette réflexion juridique vous sera utile dans vos projets.

Restant à votre écoute,

The Blockchain or in French a chain of blocks (block chain) is and remains a storage and information transmission technology. In a few words, this block chain, public or private, is above all a data base (a ledger of all operations).

However, considering the decentralized nature of this technology, it is not subject to a specific regulation or even regulation. Therefore, this block chain can be used to protect works or as a means for financial instruments: it is a new medium of trust.

In order to foster this trust, it is essential to take legal aspects into account, particularly regarding contracts, intellectual property, liability and compliance (GDPR).

As attorneys, we are confronted on a daily basis with the management of strategic issues. We help stakeholders with their legal compliance and digital transformation.


We hope you enjoy the reading and that this article will be useful for your projects.

Mathias Avocats remains at your disposal,



Garance Mathias

Avocat à la Cour



What is the Blockchain and what are its legal implications ?

For the past decade, blockchain technology hasn't ceased to expand and raise questions regarding the relation between law and technology. It is seen as the "new technological revolution" of our century. This may be explained by the fact that it offers a wide range of uses such as identity verification, recording of all type of property ownership namely real estate or Intellectual Property, automation of the contract process or near-instant money transfers. For example, the artist Imogen Heap released a song on the Blockchain and users paid to listen. The money was split on the blockchain and sent directly to the artist. Blockchain technology can adapt to any, if not all, business sectors.

Blockchain technology emerged with the cryptocurrency Bitcoin and it was the solution adopted to ensure a secure and accurate record of transactions on a peer-to-peer network. It is a decentralized technology or open ledger of information that is verified and distributed across a peer-to-peer network. Each transaction or block is recorded on the Blockchain. A transaction can only be added to the Blockchain if it is verified and validated by each participant server or computer, called "nodes". If a node does not validate the transaction, it will be rejected from the Blockchain. The validation process consists of nodes solving a highly complex algorithm.

Such technologies offer a guaranty of security. Indeed, if a transaction has

been altered or is fraudulent, the nodes will not validate the transaction and it will not be added. Furthermore, once a block has been added to the Blockchain, it cannot be altered and hacking the blockchain technology is highly improbable considering its complex cryptography and the volume of nodes and blocks. The blockchain technology warrants a secure, impregnable and self-maintaining database.

However, the Blockchain also has some deficiencies. The major concern regards the limited number of transactions which can be processed per hour. Its colossal processing power implies a certain delay which can be a problem for transactions where speed is of essence. Key legal issues also arise when considering the development and adoption of the Blockchain and other open ledger technologies. The main question is: what is the role of the law?

One of the core legal issues regard jurisdiction and applicable law. Nodes are scattered across the world and the governing law of the contractual relationship may be hard to identify. Including a governing law and jurisdiction clause will avoid this problem.

Another issue is the enforceability of smart contracts which are blockchain contracts automatically executed on the occurrence of an event. They operate as self-execution contracts even though they are not necessarily contract as legally defined. Questions may arise if a dispute must be resolved.

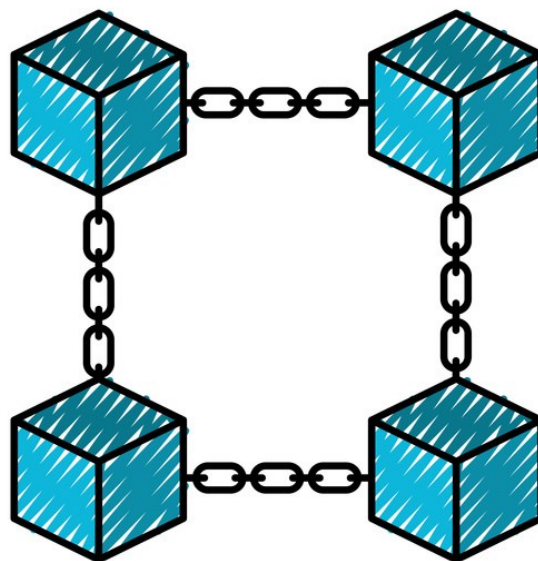
applies? Users of the blockchain technology should anticipate these issues and include adequate clauses.

A whole new set of issues arise with Decentralized Autonomous Organizations (DAOs). These digital entities operate through the implementation of pre-coded rules and the use of smart contracts. They record their activity on the Blockchain. As decentralized organizations, what are their status? The DAOs management is conducted automatically. Who is responsible if there is a breach or a violation of the law? Who or what is claimed against in the case of a legal dispute?

The European Union has other concerns in relation with the coming into effect of the General Data Protection Regulation of 27 April 2016 (Regulation n°2016/679, GDPR) on May 25th, 2018.

For a transaction taking place on the blockchain technology, can the nodes qualify as data controllers or data processors? How can individuals exercise their right of rectification or their right to be forgotten? The GDPR only allows the transfer of personal data to countries offering a similar level of protection to that in the Union. How can one certify this? A private blockchain network may be a way to ensure compliance with the regulation.

Despite these hurdles and tricky legal implications, Blockchain and other open ledger technologies are still growing and are an appealing solution to many businesses.



What are smart contracts ?

Blockchain is a diverse and flexible system. Innovative uses of blockchain technology seem to emerge frequently such as smart contracts. They have been the subject of heated debates regarding the legal issues they raise. To name just a few of these issues, what would be the applicable law? What flexibility do smart contracts offer? Is it possible to amend them?

However, smart contracts offer several advantages namely regarding automatic and regular payments such as royalties or insurance. They offer security and efficiency. Moreover, the issues raised are not new to blockchain technology. Indeed, the question of the applicable law arose when the Blockchain was first created. With a few changes in the law, just as with electronic contracts, solutions could be found.

How do smart contracts work ?

A smart contract is an encoded contract. The terms of an agreement between two or more parties are programmed into code (a set of instructions) that are stored on a blockchain technology. When certain conditions described in the code are met, specific actions, which are also defined in the code, are automatically triggered. As such, smart contracts are said to be self-executing. They operate in a comparable way to any transaction on the Blockchain.

In its analysis entitled "[How Blockchain could change our lives](#)", the European Parliamentary Research Service (EPRS) evoked the possibility of using smart contracts in the voting process. If we consider this possibility, a separate smart contract would have to be created for each election. Casting a vote would be a specific condition leading to specific actions: counting the votes and determining the election results. The instructions would determine the method for counting the votes, the limit of vote per person and so forth. It must be said that Blockchain-enabled e-voting has already taken place in Denmark and in Estonia.

Furthermore, smart contracts have also been used by the German startup [slock.it](#) which allows people to find, locate, control and rent any object through the Ethereum Computer (an open source project). If a person wants to rent an empty apartment for the holidays, he or she only has to open the application, find the apartment, pay for its use and, if the owner accepts, he or she will have access to it. The agreement between the owner and the person will be stored on the Ethereum Blockchain. The application is similar to an electronic contract. These illustrations prove the sustainability of smart contracts and the various applications they hold in today's society. They help comprehend how they function and the future purposes they hold.

What issues arise ?

In general, when referring to blockchain based technologies or Artificial Intelligence (AI), an issue commonly arises: is code prevailing on the law? Does it replace it? These questions namely refer to the “Rule of Law” doctrine developed by John Locke under which no one is above the law and the law must not be arbitrary or unpredictable.

They also refer to Professor Lessig’s article “[Code is Law](#)”. He develops the idea that code is the regulator of our cyberspace age. However, this regulator can change. The code is not fixed. He stresses the importance of understanding this regulation and the ways in which it is and may change.

When considering the Blockchain and AI, the code may seem inflexible, because it cannot easily be changed, and could appear to be “ruling” the technology it is applied to. In some ways, the code is the law of the technology.

However, when it comes to comparing code and the law, the latter holds a key place which cannot be diminished by smart contracts, the Blockchain or AI. Indeed, the law of the land sits above the so-called law of code. Despite the difficulties of enforceability and legal proceeding, the law is the ground on which decisions, interpretations and rules are made. Manufacturers as well as parties to a contract are subject to them. The law cannot be evaded.

This implies that smart contracts will most likely not replace traditional paper

contracts but offer other alternatives such as they do today. Parties to a smart contract should include particular provisions namely regarding jurisdiction and applicability.

What are the next steps?

The primacy of national law may need to be asserted in new ways to adapt to technological evolutions. Traditional contract law namely record keeping and evidentiary rules may need to be modified so as to take into account the automated nature of smart contracts. The Lord Chief of Justice for England and Wales underlined [the probable need to update the United-Kingdom’s legislation regarding these issues](#).



How can Blockchain protect Intellectual Property rights ?

As previously stated, Blockchain has expanded since its beginning with Bitcoins. Indeed, the technology is now used for contracts, music and commerce. A question has arisen regarding the use of blockchain technologies to protect Intellectual Property rights.

Some companies have already started using the Blockchain for such purposes. For example, the website [Binded](#), created by a company based in San Francisco, allows artists to protect the original images they have created. The artist must simply sign up and download his or her work. The work is then saved on the Blockchain. The artist also receives a certificate proving the authenticity of the image. However, downloading the image on the website and getting the certificate does not register the artist's work with the United-States Copyright Office. The artist will still have to comply with certain formalities to win statutory damages in a lawsuit in the United-States.

The rights attached to the work

The EPRS identified two major advantages the Blockchain offers in its analysis entitled "[How Blockchain could change our lives](#)" (February 2017): 'hashing' and 'proof of existence'.

Hashing is the equivalent to a unique digital fingerprint. It is the process by which a document is transformed into a fixed length of code. Proof of existence

is the recording of the hashes on the blockchain. These procedures apply to all transactions on the Blockchain and could be used for patents, trademarks or authorship.

If a work is recorded on the Blockchain, the creator can prove the content of the work through the hash and the time of its creation by proof of existence. Each transaction on the Blockchain is immutable. Therefore, blockchain technology offers a trustworthy proof of record. This record could be used in an infringement action to prove the copying of constituent elements of the original work and ownership.

However, the creator may have to comply with the formalities of the appropriate authority to hold his or her full bundle of rights despite the registration of the creation on the Blockchain. For example, a patent can only be delivered by the competent authority and the inventor can only claim patent rights if he or she has a patent. Nonetheless, the registration of the invention on the Blockchain will allow the inventor to protect his or her invention if another person claims to have invented the same work. The inventor will be able to prove that the other's invention is not new (a requirement for patentability).

It must also be underlined that blockchain technology could be used for unregistered Intellectual Property rights. This would namely be conveyed

nient for the fashion industry. The fashion designs are seasonal and it may not be profitable for the designers to register their rights which makes it complicated to prove ownership in an infringement action. Blockchain technology would be a fast and appropriate means to protect the designs.

Blockchain and right management

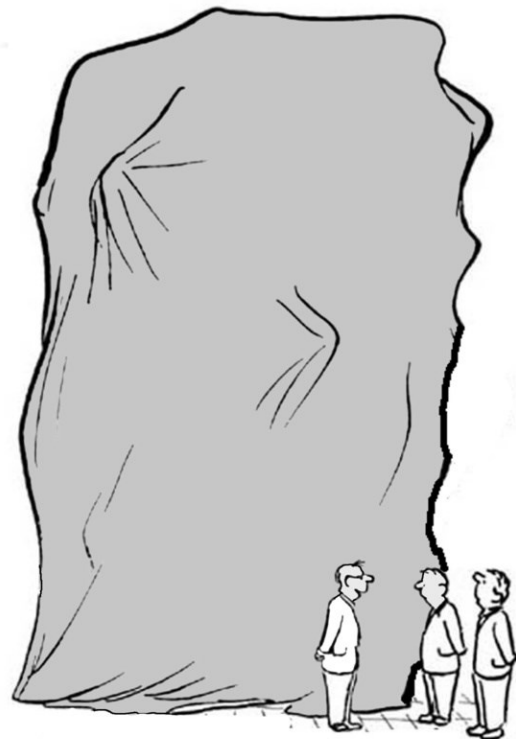
The Blockchain could also be used by third-parties or the creator to see the complete chain of ownership of a work including licenses, sublicenses and assignments. It gives more control over the work and the content of the transactions would be easily available. The Blockchain would reference all the contracts on a particular work and would enable third-parties to check that the rights acquired are legitimate.

Furthermore, the original creators of the work could use the blockchain technology for royalty payments. By digitally encoding the rights, royalty payments would become more reliable and efficient. The complex network of actors would be easily identifiable. If a suit were to arise, the Blockchain could be used as proof of the contracts and the payments made.

Conclusion

In conclusion, the blockchain technology offers many advantages for the creation and protection of Intellectual

Property rights. It is swift, inexpensive and practical. Nonetheless, in practice, such uses of the Blockchain may require reviewing the applicable legislation.



“Now, tell me about your big idea.”



How can Blockchain and trade secrets support each other ?

Let us recall that blockchain technologies are open ledgers of information which are verified and distributed across a peer-to-peer network. Simply put, it is a means of structuring data and replicating it on a myriad of computers or participating servers (nodes).

Such technologies are used in various spheres such as contracts (see Sheet n°2), Intellectual Property (see Sheet n°3), [the music industry](#) and financial sphere (see Sheet n°6). Could the Blockchain be used to protect trade secrets?

This Sheet will focus on the terms, definitions and conditions set out in [the European Union's \(EU\) Directive n° 2016/943 on Trade secrets of June 8 th, 2016](#). It must be transposed by June 9th, 2018 and harmonises the [regulations on trade secrets within the EU](#).

Article 2 of the Directive defines trade secrets as meaning “information which meets all of the following requirements: (i) it is a secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (ii) it has commercial value because it is a secret; and (iii) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret”.

How can Blockchain protect trade secrets ?

As previously stated, trade secrets must remain secret to be protected. An example of a trade secret is the Coca-Cola recipe or the algorithm powering Google's search engine. Signing a non-disclosure or confidentiality agreement may be a way of protecting them. However, the process is lengthy and may be costly (ex: lawyers' fees). Furthermore, in the event of a breach, the business must be able to prove that it had a particular concept or information at a specific time. The latter is a delicate issue.

Blockchain technologies offer an efficient and secure alternative. If a business registers its trade secrets on a blockchain technology, it will be encrypted. The trade secrets in itself will not be available to the public. The only available information is the hash which is similar to a timestamp. It can thus be used in the event of a breach. Moreover, no negotiations or lawyers are involved. The business can swiftly protect its trade secrets without any additional cost.

Under the EU's Directive, registering trade secrets on the Blockchain could be considered as a “reasonable step (...) to keep it [the information] secret”. Using blockchains technologies could be a means of protecting commercial information.

Far from a hypothetical situation, companies have started using blockchain

technologies for trade secrets. For example, [MyDocSafe](#) offers companies and individuals the possibility to protect sensitive commercial information (trade secrets) through smart contracts by using Ethereum (an alternative blockchain).

consider protecting their trade secrets as an alternative to patents or copyrights.

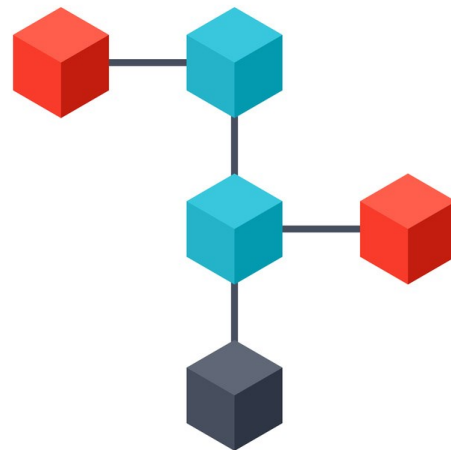
How can trade secrets protect the Blockchain ?

Blockchain can support and protect trade secrets. However, can trade secrets protect the Blockchain ?

To be protected under the Directive, the Blockchain would have to answer all three criteria set out in Article 2 of the Directive. If a business develops a new blockchain technology, the code or algorithm can be kept secret as opposed to open-source code which is available to the public. The technology would most likely have commercial value and the business would have to take reasonable steps to keep the information secret.

If each condition is met and a breach occurs, the business would have a wide range of legal remedies: damages, injunction, recall of the infringing good or the destruction of all or part of any document/object/material/substance/electronic file containing or embodying the trade secret (Articles 9 and 14 of [the EU Directive n° 2016/943](#)).

Therefore, businesses using or developing blockchain technologies should





Who is liable for the Blockchain ?

Liability is an important legal issue pertaining to the Blockchain. Who is responsible if the system fails? Can Decentralized Autonomous Organizations (DAOs) be held accountable? What law is applicable to determine liability and damages?

It must be underlined that there are two types of Blockchain. On the one hand, unpermissioned Blockchains and on the other hand permissioned Blockchains. The former is open to anyone whereas the latter is maintained by a limited group of actors which retains power to access, check and add transactions to the ledger. Permissioned Blockchains are less transparent than unpermissioned Blockchains and are decentralised. They raise different issues. Despite their differences, both blockchain ledgers operate in the same way.

Permissioned and unpermissioned blockchain ledger

DAOs are a new form of legal structure in which ownership, management and control are automated and human intervention is limited. They can be understood as a bundle of smart contracts by which a set of governance rules are automatically enforced and executed through the Blockchain. They are similar to control authorities in the sense that they set the rules governing the transactions on the Blockchain.

However, as a new form of legal structure, they have yet to be defined. Are


DAOs corporations or are they something else? Without a precise definition, it is arduous to determine an applicable regulation. Moreover, what, if any is their liability? What about the liability of the creators of DAOs? Who is claimed against in the case of a legal dispute? The issues have yet to be addressed.

One of the significant issues affecting public blockchain ledgers is the inability to control and stop its functioning. If a person decided to sell illegal products, how can the illegal business be brought down? For example, if DAOs were programmed to trade illicit goods or banned products, it would be difficult for victims to recover damages or to obtain an injunction against the malicious DAO unless it were programmed for such cases. And, if this were the case, what about the programmer's liability?

Another problem arises regarding identity. Although other people on the Blockchain see a person's public key and his or her name, anonymity is still a possibility. If this is the case, and a person suffers a damage, but cannot identify the alleged wrong-doer, how can a remedy be awarded?

These concerns have also not yet been addressed.

The issue of liability is not as controversial for permissioned Blockchains. Seeing as only a pre-selected group can add transactions to the ledger, the identity of the persons in the group is



more readily assessed. If a harm were to occur, both persons could settle and go to court because they know who they are.

The general issues of liability

For both types of blockchain ledgers, jurisdiction and the applicable legislation must be defined prior to any transaction. What law is applicable for liability? Which court has jurisdiction? Providing specific provisions for these issues could be a solution. However, considering the varying complexity of the Blockchain and the fact that it has no geographical limitation, such provisions may be difficult to draft.

Generally, if a problem were to occur in the Blockchain, who would be responsible? The owner? The developer or programmer? The malicious person?

Furthermore, a question arises as to the applicable contractual law for transactions. Which law is to be applied? If the contract is wrongly encoded, how can it be changed? Are amendments possible? Regarding transactions, what is the legal status of the users? Are they consumers? Must they be professionals when providing specific services (financial services for example)? What protection can they claim?

If a user steals a private key, which is unique to each user and can be defined as the encrypted identity card of a user, how can it be proven? The frau-

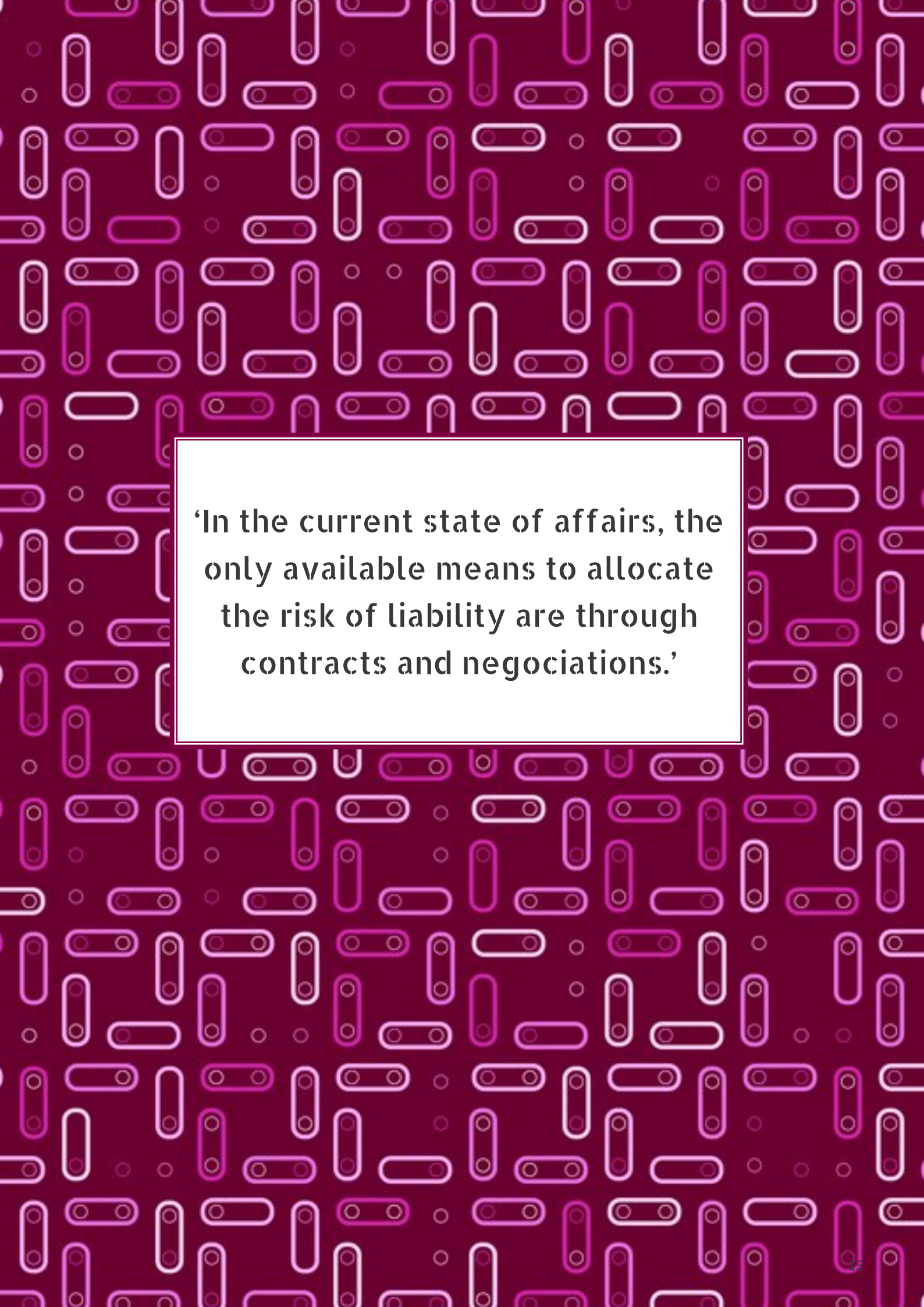
dulous transactions could not appear as such and be validated. If several private keys are stolen, the Blockchain is no longer secure. How can users be warned? How can the Blockchain be secure again?

What is the outcome ?

In conclusion, the Blockchain raises many concerns. Answers have yet to be found.

Current legislations and regulations are not necessarily fit or adaptable to a blockchain ledger. Nonetheless, the allocation and attribution of risk and liability in relation to a malfunctioning blockchain service should be careful though thorough.

In the current state of affairs, the only available means to allocate the risk of liability are through contracts and negotiations. The contract should namely consider the imminent coming into force of the GDPR to which the Blockchain could be subject. It should also address Intellectual Property issues.



‘In the current state of affairs, the only available means to allocate the risk of liability are through contracts and negotiations.’



What is an Initial Coin Offering (ICO) ?

ICO has become a popular term in the legal and financial spheres. It is defined as an [unregulated issuance of digital assets where investors can raise money in cryptocurrencies](#). As opposed to an [Initial Public Offering \(IPO\)](#), an ICO is strictly restricted to cryptocurrency and is unregulated. It can be considered as a form of crowd-funding.

This flexible funding mechanism attracts an increasing number of companies. According to [a Goldman Sachs study](#), since June 2017, ICO fundraising has surpassed seed and angel funding as the main source of technology funding.

ICOs are linked to the Blockchain to the extent that the latter can be used for financial transactions and namely cryptocurrencies. Let us recall that Blockchain emerged with the cryptocurrency Bitcoins.

How does an ICO work ?

As previously stated, an ICO is a funding mechanism for companies. As such, it must be carried out during the project's start-up phase. The terms of the contract and the project will be outlined in a white paper made available to the investors.

In practice, during an ICO, an investor will acquire digital assets called tokens and the company will obtain cryptocurrencies to fund its project. It must be underlined that tokens are not

shares of the company and do not entitle the investor to any sort of cash flow (ex: dividends). Thus, tokens do not give ownership rights. Tokens are rights in the company's project and will vary according to the purpose defined (ex: money transfer, registry, services...).

Nonetheless, investors should be forewarned of certain risks. This is all the more important seeing as investors can be laymen. They will not have the same business knowledge as professionals and may be more vulnerable. For the company launching the ICO, the lack of professionals may also dampen the project's rate of success considering the lack of contacts or experience of laymen investors.

The lack of regulation for ICOs leads to legal uncertainty. If ICOs are not legally qualified, how can an investor protect him/herself? What action(s) can be brought? In the event of a scam or hacking, what remedies are available?

In practice, investors should check the compatibility of the tokens with their wallets. Indeed, certain wallets may be incompatible with the tokens bought. Investors should consider having a wallet which allows the export of private keys in order to be able to transfer the tokens to a new compatible wallet. Furthermore, some trading platform may not accept all tokens. This makes it harder to invest and make a profit.

Can ICOs be regulated ?

Recently, there has been a growing concern regarding the lack of regulation for ICOs. Several countries have taken initiatives to protect investors and to set up ground rules for companies launching an ICO.

For example, the Securities and Exchange Commission (SEC) of the United-States has taken several steps to regulate ICOs and protect investors. The Commission namely created a [Cyber Unit](#) which will focus on targeting cyber-related misconduct such as violations involving distributed ledger technology and ICOs. It further published [an Investor Bulletin on ICOs](#) providing guidance and explanations. The Bulletin also provides that certain tokens may qualify as securities subject to the SEC's jurisdiction.

The European Securities and Markets Authority (ESMA) is also considering the subject. It recently issued [two statements on the risks ICOs for investors](#) and [firms](#). Other countries have yet to take initiatives and some have imposed bans on ICOs (ex: [China](#)).



Blockchain and the GDPR : how do they interact ?

The GDPR which comes into effect on May 25th 2018, will have significant impacts on personal data protection legislation. In this regard, questions have arisen regarding the relation between the Blockchain and the GDPR.

Let us recall that the Blockchain is a decentralized technology or open ledger of information that is verified and distributed across a peer-to-peer network. It is composed of a set of nodes which are similar to registrars. Each node holds personal data pertaining to each participant server or computer.

Therefore, Blockchain allows the flow of data from one person to another in a secure, flexible and convenient manner. How is personal data on blockchain technologies protected? Will they be subject to the GDPR? How can blockchain technologies and the participants be characterised under this new legislation ?

Is the Blockchain subject to the GDPR ?

The first question which comes to mind is whether blockchain technologies are subject to the GDPR.


For the Regulation to apply, there must be a processing of personal data. Processing activities are "any operation or set of operations which is performed on personal data or on sets of personal data" ([Article 3, 2° of the GDPR](#)). Personal data means any infor-

mation relating to an identified or identifiable data subject ([Article 3, 1° of the GDPR](#)). The nodes on the Blockchain are digitally signed by the participant and the signature is a means of identification. It is personal data. The latter is collected, recorded and stored on the Blockchain. As such, it processes personal data and may be subject to the GDPR.

Furthermore, the Regulation has a large territorial scope. Indeed, in a few words, the Regulation will apply when the controller or processor is established in the European Union (EU) or when the processing activities relate to data subjects in the EU.

This leads to another question: who are the data controllers and/or processors? The controller is the legal or natural person who determines the purposes and means of the processing of personal data whereas the processor is the legal or natural person processing the personal data on behalf of the controller ([Articles 4, 7° and 8 of the GDPR](#)).

Regarding the Blockchain, miners, the persons confirming the transactions and writing them into the ledger, could be considered as joint data controllers. They process the information in the node. However, this characterisation is not fully satisfactory considering the fact that computers accomplish most of the processing. Miners could also be characterised as processors.



The GDPR also sets out certain conditions for the lawfulness of processing personal data ([Article 6 of the GDPR](#)). What legal basis could be applied to blockchain technologies? Can the participant be considered as having consented? Is the processing necessary for the performance of a contract to which the participant is a party? Is the processing necessary for the purpose of legitimate interests pursued by the controller? These questions have yet to be answered and have also been raised regarding liability (see Who is liable for the Blockchain?).

Can the Blockchain protect the rights of data subjects ?


Under the Regulation, data subjects hold certain rights such as the right to rectification ([Article 16 of the GDPR](#)) and the right to erasure ([Article 17 of the GDPR](#)). The immutability of the data on the Blockchain seems to counter these rights. If the code cannot be changed or amended, how can the data subject rectify or have his or her data erased?

It could be argued that nodes could be changed either by a court order or by the miners. However, this situation raises another set of issues pertaining to the integrity and security of the Blockchain. Nodes are verification means. If one were modified or deleted, what impact would this have on the chain?

Data subject also have a right to be informed about the data processing. How can this be done through the Blockchain? How can the Blockchain ensure transparency? If these conditions are not met, a data subject cannot give informed consent.

Furthermore, data subjects may also have the right to be informed of a data breach if it is “likely to result in a high risk to [his or her] rights and freedoms” ([Article 34 of the GDPR](#)). How can a data controller inform a data subject of a data breach on the Blockchain? What system could be put in place? What measures could the data controller subsequently take if the code is immutable? The same hurdle must be overcome for the notification of personal data breaches to the supervisory authority ([Article 33 of the GDPR](#) and [WP29 guidelines on Personal data breach notification on October 3rd, 2017](#)).

Another issue arises regarding Data Privacy Impact Assessments (DPIA). The controller must carry out a DPIA when the processing is “likely to result in a high risk to the rights and freedoms of natural persons” ([Article 35 of the GDPR](#)). The WP29 clarified this obligation in its [guidelines regarding the data protection impact assessment on October 4th, 2017](#). A DPIA will namely be mandatory for large scale processing activities. The Blockchain falls within this category.



However, is it possible to carry out a DPIA of all transactions on the Blockchain? How can a controller determine the scope of the DPIA? Will the risks be the same for all data subjects? If data processors cannot be qualified on the Blockchain, are there other means to fulfil this obligation? The DPIA is of particular importance to prove conformity with the GDPR and with the principle of accountability.

Can data transfers on the Blockchain be conform to the GDPR ?

Blockchain technologies have no geographical limit and data can transfer quickly across the world. This is one of the major assets of the Blockchain. However, this asset may become a hurdle under the GDPR. The later provides that personal data transfers may only occur if the other country conforms to the Regulation and presents a similar level of protection or appropriate guarantees ([Articles 44 to 49 of the GDPR](#)).

How can one determine in which country the other participant is? How can the Blockchain ensure that transfers only occur in countries with a sufficient level of protection? Or, could blockchain technologies be considered as providing a similar level of protection?

There are various means of providing appropriate grantees such as standard contractual clauses or binding corpo-


rate rules. Could standard contractual clauses be defined in regard to transactions on the Blockchain? How could one access binding corporate rules? Could an approved certification mechanism be appropriate?

Sum up

It is important to note that most questions arise with un-permissioned Blockchains. The latter are open to anyone whereas permissioned Blockchains are maintained by a limited group of actors which retains power to access, check and add transactions to the ledger. Seeing as each participant is identified, most issues presented in this article are more easily resolved.

One must bear in mind the lack of State regulations regarding these issues. Participants on the Blockchain must rely on contractual law. Blockchain technologies offer a new means for transactions which operate just as any other transaction and, as such, are subject to a contract. Indeed, there is an offer, acceptance, consideration, mutuality of obligation, competency and capacity.

In this context, participants must be particularly vigilant and keep in mind that the transaction answers to contractual law and the obligations they define. Once again, permissioned Blockchains offer a significant advantaged with the limited group of actors.



New regulations for the Blockchain ?

With the rise of ICOs and of innovative technologies relying on the Blockchain, the issue of regulation has become crucial. It appears that countries have taken initiatives to draft regulation within the financial sphere. The Securities and Exchange Commission (SEC) of the United-States has namely created [a Cyber Unit](#) which will focus on targeting cyber-related misconduct such as violations involving distributed ledger technology.

In France, the government recently passed the [executive order n°2017-1674](#) concerning the use of a shared registry system, namely the Blockchain, for the representation and transmission of financial securities. The wording “shared registry system” was carefully chosen to include any future similar processes similar to the Blockchain.

It is the first regulation to define a legal regime adapted to the transfer of ownership of financial securities through the Blockchain making France the first financial center of the European Union.

Blockchain technologies can be used for financial transactions or cryptocurrency. The Blockchain emerged for and with [Bitcoin](#). It ensures traceability and security seeing as each node must verify and validate prior transactions. If a prior transaction is not validated, the transaction will not go through.

This Sheet draws an overview of the executive order and the impacts it will have.

What financial securities are concerned ?

The extensive scope of the executive order is negatively defined. It specifically targets all financial securities falling outside the scope of services Central Securities Depositories (CSDs) can provide.

Under [Article 2 of the EU Regulation n° 909/2014](#), a CSD is a legal person that operates a securities settlement system (settlement service) and either provides initial recording of securities in a book-entry system (notary services) or provides and maintains securities accounts at the top tier level (central maintenance service).

Thus, the executive order covers all other financial securities or transactions and namely:

Marketable debt instruments – units or share of collective investments undertakings – Capital securities issued by stock companies and other debt securities under the condition that they be unlisted.

What does this imply in practice ?

The executive order amends [the Monetary and Financial Code](#) as well as [Article L. 288-1 of the Commerce Code](#). It incorporates “shared registry system”

as a valid means of registry. Thus, the registry of issue or trading of securities on a shared registry system will have the same legal effect as the entry of financial securities in an account.

It must be underlined that the executive order does not create any new obligations or conditions. However, the existing guarantees relating to the representation and transfer of financial securities must still be respected.

In practice, professionals and laymen will be able to use shared registry systems, namely the Blockchain, for their financial transactions or operations and benefit from the protection of the law.

The executive order will come into force, at the very latest, on July 1st, 2018. The Council of State (Conseil d'Etat) must still issue a decree detailing the applicable conditions to the registration of financial securities on a shared registry system.



“Uh oh, here come more regulations.”

**You can subscribe to our Newsletter on the
firm's website:**

www.avocats-mathias.com



About Mathias Avocats

We are a law firm with a focus on organisations being changed by technology and the digital world.

Our clients include some of the largest financial institutions, and leading technology companies. We also represent investment funds and startup companies, and over the years have supported many in their growth and development as leading industry players and household brands.



Do you have a question ?

A team dedicated to achieve your ambitions will reply :

01 43 80 02 01

contact@avocats-mathias.com

19, rue Vernier – 75017 – Paris

Find our lawyers' practical advice on Twitter :

[@GaranceMathias](https://twitter.com/GaranceMathias)

