MINISTRY OF CULTURE AND COMMUNICATION, FRANCE

—

CONSEIL SUPERIEUR DE LA PROPRIETE
LITTERAIRE ET ARTISTIQUE

Report of the mission assessing the state of play for *blockchain* and its potential effects on literary and artistic property rights

Leaders of the mission: Jean-Pierre Dardayrol and Jean Martin
Rapporteurs: Charles-Pierre Astolfi and Cyrille Beaufils
Report translated by Cultures Connection

Report submitted to CSPLA on 13 February 2018
Its content reflects the views only of its authors

January 2018

Foreword by leaders

Dialogue with representatives of writers and creative industries, conversations with businesses and high-tech start-ups, wide-ranging research and thorough analysis by the rapporteurs have resulted in this report assessing the current state of play for *blockchain* and its variants.

Readers will find an abundance of verified material here; more than that, they will also certainly find material for reflection and for forecasting, according to their own situation, history, environment and aims.

For preparation of these important and demanding undertakings, the leaders of the mission wished to provide their own forward-looking view, in a few simple, brief points, on completion of their mission.

We do not know what *blockchain* is going to become, but it will exist in many forms (it would be more appropriate here to talk about *blockchains* to take into account the diverse concepts and implementations which will be successful, among many failures).

In its current form, *blockchain* technology does not meet the requirements of literary and artistic property law.

Participants in cultural industries, and their audiences, form an information system, through their creative, production, distribution and operational actions, a system which is constantly changing and aiming for optimisation, for many reasons, including economic efficiency and development of new products and services, as well as to respond to changing social practices and technical opportunities.

Blockchain is a multi-functional system for managing information which, depending on configurations and applications, aims to provide security, transparency, immediacy and automatic implementation of operations, for an infinitesimal cost.

It would be somewhat surprising therefore that these two worlds were not engaged in fruitful cooperation, just as it would be risky not to take active preparations given the increasing rate of development and deregulation.

Thus it seems vital for the cultural industries to participate in this movement, especially with partners, first and foremost so they are not left behind among the losers.

There are two possible aims for taking part in this process, complementary but differing in their methods, strategic challenges and the timetable for achieving them: on the one hand, optimisation of management (in terms of costs, or deadlines, or quality, etc.), and on the other, innovation of models (social, economic and more).

At the moment, the search for opportunities includes, among other things, on the one hand building links between the physical world and the digital world (see “oracles”), and on the other, traceability (of practices, objects, etc.).

The cultural and creative industries have a limited window of opportunity in this field at the moment, to take the initiative in a context marked by ubiquitous and widespread “production” and “consumption” practices, as well as by the combined new waves of innovation in information technology (big data and artificial intelligence in particular).

Report

Before becoming a transformative, even a creative technology for new business practices or models, *blockchain* was a focus of interest. From its first steps within a community of initiates, to its legitimization on the cover of *The Economist*, this concept has intrigued or converted many players, some of whom are beginning to offer innovative services, tools or practices using this technology, outside the context of its initial application, which was the creation of a digital currency.

The essentials of *blockchain* are focused on two pledges: being able to create "digital property instruments", and allowing these to be exchanged without the need for a central authority. What these property instruments cover exactly is up to the users, who can invent their own business practices and models with them.

The initiatives, the many start-ups and industries gathering around this technology are gradually constructing and enhancing their technical concepts, business models, sectors and distribution centres with technical, legal and managerial skills; cultural industries are no exception. However, the most varied players are starting to discover the potential for transformation, globally, finding that *blockchain* offers them usages relevant to their own operations, and even that it offers a necessary boost to the development of innovative projects.

Table of contents

While since ancient times, the character of Prometheus in chains has symbolised technical progress, today it is the chains themselves, chains of blocks, or *blockchains* – which are offered as an innovation that can improve or call into question the models used by historic players in many economic sectors or public authorities.

Called the "Trust machine"[1], *blockchain* is an innovative use of known technologies, whose complexity gives it a mythical status. Some of the pledges and warnings proposed regarding its development sometimes rely on an inadequate understanding of its capabilities and current limitations, as well as its current or future developments.

Properly understood, *blockchain* does indeed bring real benefits in terms of efficient, secure transactions and exchange of data, as the many players who have adopted the technology realise, learning about its full potential through pilot applications, sometimes shared with other users.

While some participants in cultural industries are already involved in this dynamic field[2], the primary aim of this report is to awaken the interest of CSPLA members in this technology and give them the initial keys to reflect on its potential effects in their sector, and on literary and artistic property, and where applicable, to engage in pilot schemes or tests.

The Economist, 31 oct. 2015

2 https://societe.sacem.fr/actualites/innovation/les-blockchains-une-opportunite-economique-pour-le-droit-dauteur

1. Emerging technology with development potential

Blockchain was invented in 2008, as the brief history included in the appendix to this report describes, but its applications beyond that of virtual currencies have been perceived more recently. At the end of 2015, the British weekly *The Economist* was already able to introduce a number of initiatives taken by economic players, mainly private businesses at that time, to experiment with applications for *blockchain* in their sectors. The consortium of almost 70 banks, associated with the *start-up* R3 CEV, to carry out shared research on this topic in the field of interbank transactions, was the best example of this at the time.

The interest in the technology then increased to include States concerned to make their land register more reliable, for instance, or secure the exchange of medical data, as well as luxury goods companies and diamond merchants wanting to ensure traceability of their products. Several pilot schemes were started for this, and made public.

In France more recently, the Caisse des dépôts, as part of the *ad-hoc* consortium LaBChain, and the Banque de France, brought together various players around pilot schemes, for issuing SEPA creditor identifiers, in order to understand how *blockchain* works, and to consider the legal and managerial questions raised by its use.

Aside from these practical initiatives, *blockchain* also arouses the interest of public authorities, and the first attempts to include it in regulations. So for instance, in 2016 the State of Vermont in the United States recognised the legal force of *blockchain* evidence following a joint report from its Secretary of State, its public prosecutor and its commissioner for financial regulations.[3]

At the same time, *blockchain* also appeared in French law. For instance, since April 2016, the French Monetary and Financial Code[4] has included the option of recording transactions relating to 'minibons' [cash receipts] in the form of a *"shared electronic registry device*", thus adding *blockchain*, under this designation, to the legal corpus. Similarly, article 120 of the "Sapin II" Act[5] has authorised the Government, by means of an order[6], to take the legislative steps needed to "*adapt the law applicable to financial instruments and transferable securities in order to allow the use of a shared electronic registry device to represent and transmit securities which are not accepted in the operations of a central securities depository, nor supplied in a system for control and delivery of financial instruments*", which led the directorate of the French Treasury to launch a public consultation to gather the views of players in the financial markets about this topic[7].

3 James Condos, William H. Sorrel, Susan L. Donegan, "Blockchain Technology: Opportunities and Risks", 15 Jan 2016James Condos, William H. Sorrel, Susan L. Donegan, "Blockchain Technology: Opportunities and Risks", 15 Jan 2016

4 Art. L. 223-12 CMF: "*Without prejudice to the terms of article L. 223-4, issue and transfer of minibons may also be included in a shared electronic registry device, allowing such operations to be authenticated, under conditions, particularly those regarding security, as defined by a decree in the Council of State."*

5 Act n° 2016-1691, 9 December 2016, relating to transparency, the fight against corruption and modernisation of economic life .

6 Order n°2017-1674 8 December 2017, relating to the use of a shared electronic registry device for representation and transmission of securities.

7 see also the consultation launched by the European Securities and Markets Authority (ESMA) on the same subject, on 2 June 2016:

2. The two functions of *blockchain*: registration and transfer

Without going too soon into great detail about the functional and technical characteristics, which are covered in the appendix to this report, the value of *blockchains* can be summarised by saying they allow information to be stored and transferred securely, without recourse to a central organising body.

The information contained in the *blockchain* consists of encrypted summaries of transactions, called *hash*. [8]

So the *blockchain* holds the register of the transactions between its users, allowing them to exchange "virtual property certificates" (also called tokens), and only they can claim the resource symbolised by the certificate they hold. It is the use and consensus among users of a particular *blockchain* which define what these certificates represent; a certificate may represent a unit of currency, but also for instance ownership of a financial asset.

By holding this register of transactions, the *blockchain* allows its users to exchange such certificates independently of any centralising body, by respecting several guarantees:

- *transfer of ownership*: when a user transfers a certificate they own, they lose control of it, and it passes to the recipient;
- *authentication*: only the owner of a certificate can transfer it;
- *unalterability*: it must not be possible to cancel or modify a transfer after the event; passing a certificate back to its original user will assume a second transfer, rather than cancellation of the first;
- *transparency*: all transfers must be public, and must be open to inspection by all, or by a private group.

As it records encrypted summaries, the *blockchain* also allows the track of a digital content (text, music file, etc.) to be preserved, by registering the summary of this content at a given moment. It also allows automation of transactions between its users.

The main uses and functionalities of the *blockchain* result from these means of operation.

8 For instance, the encrypted summary of this phase, by the SHA-256 algorithm, is this sequence of 64 characters: 2e04f10f6569204b7de740cfdb797c4ea239c4c837c6d9692fe3b30dbb4def5a

3. Functionalities

Blockchain allows information to be recorded quickly (around a few minutes on the main *blockchains* today), in a secure, distributed way. It therefore has many advantages in applications used today which depend on lengthy and more costly processes for this kind of recording.

In general, these benefits are:

- saving time;
- automating processes
- reduction in costs, because of faster processes and less use of the technical and human resources needed;
- better security;
- greater transparency.

Aside from these features, the value of *blockchain* is certainly better appreciated by describing the three main situations, or use cases, where it has proved to be especially relevant. These are:

- recording transactions;
- proof of authenticity;
- automatic contract fulfilment.

3.1. Transactions on *blockchain*

The primary function of *blockchain* to support transactions is mentioned in the previous section, and described in detail in the technical annex about the virtual currency exchange model.

This is certainly the most obvious use of *blockchain*, since it relates to essentially digital or intangible assets (virtual currency), sometimes long-dated (securities), for which one of the trickiest of the other use cases, regarding the link to the physical world, is not present. Using the mechanism of these certificates however, *blockchain* can also be used to record digital transactions which reflect exchanges in the physical world: just as today, for the sale of a motor vehicle to be valid its registration document has to be transferred, we could imagine that this function might in future be provided by transferring the corresponding ownership document to the vehicle in *blockchain*.

3.2. Proof of origin and traceability

The second major use case of *blockchain* consists in using it not as a means to record a transaction between two parties, but as a register for a person to establish the precedence of their rights over or action on an object, and thus to track how it develops.

As part 2 of this report has explained, *blockchain* records the *hashing* of transactions, in a public and irrevocable form – unless the *blockchain* is corrupted. Rather than being a summary of a transaction, however, the *hash* registered may also correspond to a written

document. A document of several hundred pages, or a contract, can thus be *hashed* then inserted into the *blockchain* at a particular moment. With a document or contract, another user can then check it matches precisely the one recorded in the *blockchain* on that date. If the text the user has differs by even one letter from the original, the corresponding *hash* will be completely different from the one published on the *blockchain*.

A bit like a modern version of the postal franking placed on a sealed envelope, the *blockchain* is thus a way to guarantee the existence of a particular document on a given date. Conversely, it is important to note that registration in *blockchain* does not in any way guarantee the veracity of the information contained in the document. This content is only worth the trust placed in the person who wrote and registered it. Moreover, because of the way *blockchain* encryption works, there is no guarantee against identity theft: someone managing to obtain another person's private key can sign any transaction on the register in the owner's name.

One final limit on its use relates to the fact that *blockchain* does not allow the document itself to be recorded, only its *hash*. The original electronic version, from which comparison should be made, must be kept elsewhere, which assumes availability of sufficient data storage capacity. This means, conversely, that simply reading the *blockchain* does not disclose the content of the document, so its confidentiality is protected.

3.3. Automatic contract fulfilment on *blockchain*

The final main use of *blockchain* arises from its ability to act as a support for *smart contracts*, automating contract fulfilment.

Smart contracts are computer programmes which respond to the activation of a condition ("if a natural disaster occurs"), leading to a result ("then €10,000 will be transferred from the insurer's account to the insured party's account"). Recording such "contracts" in *blockchain* allows them to be automatically fulfilled if the condition is met - for instance, when the result involves an exchange of virtual currency - and on the other hand, to ensure they cannot subsequently be altered.

These smart contracts may form either a transcription in the *blockchain* of the conditions for executing a contract existing elsewhere, or represent the contract themselves, if they are the only evidence of the exchange of intention between the parties.

They may also be fairly complex, especially if they involve other smart contracts, in a kind of chain reaction. Decentralised, autonomous organisations (DAO) have been designed on this model. They involve an investment fund, whose rules of operation (voting on investment plans, re-investment of dividends, etc.) have been automated and entered in the *blockchain*. The Slock.it start-up has, for example, launched "The DAO", a programme to raise almost 55 million dollars, using the Ethereum *blockchain*. This ambitious programme also proved fragile, because the smart contract code contained a flaw which was exploited by a hostile player to steal one third of the funds.

Reaction to this theft also illustrated the problems of governing *blockchain*: while some users considered the "contract" code had the force of law, and the theft carried out was therefore legal, another group preferred to return to a status of the *blockchain* prior to the

theft, by creating a “fork” in the history, but thus calling into question the cardinal principle of irrevocability of the *blockchain*.

This incident proves that this third use of *blockchain*, promising though it may be, has to be addressed with the usual caution for this type of information system, On the one hand, the quality of the computer code needed must be guaranteed, as in any application. And above all, from a legal point of view, this usage does not allow for some questions to be raised, especially about its interaction with conventional contract law. While the agreements do have the force of law between the parties, they still rely on the goodwill of both sides to ensure their fulfilment, and in most cases need a judge to intervene when either party has to be forced to meet their obligations. On this occasion, the judge may review the contract and ensure, for instance, that it does not involve an illicit matter, or does not contain an unconscionable clause. On the other hand, as the smart contract automatically executes the contract, the judge's role will probably involve “cancelling” this execution at the request of one of the parties, after the event. It remains to be seen how this intervention will work with two of the founding principles of *blockchain*: the absence of trusted third parties - how is the “legitimacy” of the judge's decision recognised in this context, and its executory force ensured? - and irrevocability.

In addition, when the condition triggering execution of the smart contract is linked to the physical world, such as in the example of a natural disaster triggering an insurance payout, the intervention of an “oracle”, responsible for ensuring this condition is fulfilled, will be needed to make the link between the physical world and the *blockchain*.

It is no doubt for such reasons that use of smart contracts may be considered more suitable for establishing relationships between objects, particularly in the context of the internet of things. A driverless vehicle may thus refuel at a petrol pump, with a smart contract triggering payment when the tank is full.

4. Potentialities mobilised, examples from the sectors

4.1. Technology applicable to many sectors

The most elementary use of a *blockchain* consists of creating a currency. This currency may then be exchanged within the blockchain, or against other currencies (virtual or not) via exchange platforms.

Other uses are planned or suggested: for instance, a certificate may represent proof of ownership of a work of art, whose successive resales would be represented by an equivalent number of transactions on a *blockchain*; this would allow a potential purchaser to check the history of all transactions of the work back to the first one, to ensure its authenticity (for instance if the first transaction came from the artist or the artist's agent), or the amount of each sale (if this is made public).

The abstract nature of virtual certificates means there is potential for any number of uses and options, depending on what such securities are linked to outside the *blockchain* to which they belong. This is the context in which users of a particular *blockchain* apply it for a particular community, as the blockchain concerned provides a digital, incorruptible "ledger", complete and always up to date, but itself not forming the link with its context for use.

4.2. The *blockchain*, support for virtual transactions: applications in the world of finance

With regard to these initial applications, the sphere of financial transactions was naturally the place for the first experiments with *blockchain*.

Banks were among the first to show interest in this technology, especially for its back office use, regulating transactions between banks. While at the moment *blockchain* seems unlikely to replace consumer payment methods such as bank cards in the short term, given the time needed to register a transaction (a few minutes with the Bitcoin and Ethereum *blockchains*) and its cost (a few cents for Bitcoin), these very features are a real advantage when it comes to using it for reconciliation of interbank transactions, such as buying and selling securities, particularly those unlisted, or international transfers, the time for which (two to three days) and the cost (several tens of billions of dollars annually for managing securities exchanges) would be significantly reduced. Use of a shared register also avoids having two separate sets of accounts, one in each of the banks which are party to the transaction, overcoming the inconsistencies which inevitably arise between the two. Financial institutions thus hope to increase their efficiency, with lower operating costs, thanks to the reduction in human resources needed for back office work, as well as by reducing the counterparty risks. Blockchain can thus replace clearing houses, or make them much more efficient.[9]

While applications in the financial world are still in essence at the "proof of concept" stage, there are two examples which can certainly focus the interest of this sector more sharply on *blockchain*. In August 2016, Bank of America Merrill Lynch, HSBC and the Singapore Infocomm development authority produced an application for issuing letters

9 For a more extensive list of the potential benefits to the finance industry, see the ESMA consultation mentioned above

of credit, used for funding export trade, via *blockchain*.[10] This is used to allow each of the four parties concerned - the exporter, the importer and their respective banks - to approve the transaction in turn, and monitor its progress.

Similarly in France, the consortium of banks and insurance companies, led by the Caisse des dépôts et consignations, tested the use of *blockchain* in November 2016, at the boundary between transactions and smart contracts, for managing margin calls for collaterals in securities lending.[11] Here, *blockchain* has the task of acting as a financial *middle-office*, performing a single calculation for the value of the margin call between the two institutions concerned.

4.3. *Blockchain*, proof of authenticity: example of tracking valuable goods and documents

Several applications have been developed aiming to prove authenticity of an item, from its origin, and together with the transaction function, tracing the history of this item through its various stages, where necessary. *Blockchain* thus has evidential value here.

For example, the *start-up* Everledger[12] has registered over one million diamonds since its creation, using *blockchain*. In a sector where guarantee of legitimate origin is key - as against "blood diamonds", synthetic diamonds and insurance fraud - *blockchain* can register a diamond using around forty characteristics (colour, weight, transparency, etc.). The buyer of a diamond can then be assured it has been properly registered from the outset as coming from a legal mine in South Africa, for instance. *Start-ups* are proposing to extend this use to other sectors in which the fight against counterfeiting is important, such as drugs and luxury items or even tracking containers in international trade.

The use of blockchain as proof of authenticity can also be exploited for supporting documents with significant value. This could include civil status certificates, diplomas or ownership documents. Several states, including Honduras – which appears to have subsequently abandoned the project [13] –, Ghana[14] and Georgia[15] have launched experiments involving their land registry, authenticating ownership documents using *blockchain* to ensure they are not modified later, by a corrupt official for instance. Similarly, Estonia has adopted the Keyless Signature Infrastructure system, developed by Guardtime[16] to certify various administrative documents, including eventually the medical records of around one million patients.

10 "BofAML, HSBC, IDA Singapore Build Pioneering Blockchain Trade Finance App", 10 August 2016, press release from HSBC "BofAML, HSBC, IDA Singapore Build Pioneering Blockchain Trade Finance App", 10 August 2016, press release from HSBC

11 *Agefi*, 4 nov. 2016

12 https://www.everledger.io/https://www.everledger.io/

13 Blockchain Land Title Project 'Stalls' in Honduras", *CoinDesk*, 26 Dec 2015

14 http://bitlandglobal.com/http://bitlandglobal.com/

4.4. *Blockchain,* underpinning smart contracts

Aside from the example of weather-related insurance, and the unfortunate one of "*The DAO*" already mentioned[17], several smart contracts applications are possible. In France, they are still at the project or experimental stage at the moment.

An example similar to that of insurance would be a smart contract for betting: achievement of the condition (a win for a horse or a football team, for instance) would trigger a financial transaction between two parties to a bet, or between the punter and the bookmaker.

More innovative still would be the business-object example. The researcher P. de Filippi has developed a "plantoid"[18], halfway between a robot and an artwork, which solicits the generosity of its admirers, collects their payments via the *blockchain* then launches calls to tender for creation of new plantoids. Similarly, a car or an apartment could lease itself to individuals, receive payments, order and receive supplies or repairs via smart contracts, etc.

17 On this, see part 3.3

L'Echappée volée, 28 May 2016

5. Opportunities for the world of culture

5.1. Opportunities to be developed for cultural industries

Blockchain probably has numerous use cases which have not yet been explored, or even imagined. The examples mentioned in the previous section all form part of a phenomenon which is more than just *blockchain*: automation and removal of intermediaries in processes and practices which up to now have often been centralised (such as currency transfer, which needs to pass through the banking system), or those which were not even possible without a central authority (such as creation of currency which historically has always been supported by a central bank, or a resource which was available in limited quantities, such as gold).

In cultural industries, the sometimes very large number of players in the value chain of a cultural product, and the complexity of dealing with them, for instance, in relations with stakeholders, may be fertile ground for initial applications with a *blockchain*. This dynamic would then allow efforts to be focused on activities with a high added value: legal advice, distribution strategy, partnership negotiations, while leaving *blockchain* to deal with the parts more suitable for automation, such as identification, payments and calculation of fees payable to stakeholders.

Beyond these examples, and those mentioned in the previous section, the movement initiated by *blockchain* will not stop at the threshold of the cultural industries: it will create new practices, and greatly modify existing practices in these industries, at all levels of the value chain, from consumer to creator. So the challenge for those in the world of culture is to identify services (existing or not) which a *blockchain* could support, learn from feedback in Europe and around the world, and on this basis, undertake pilot schemes, either collective or transnational as appropriate.

5.2. Some examples of existing uses:

5.2.1. Blockchain supporting transactions

In the literary and artistic property sector, the use of *blockchains* as a transaction support is also possible, whether between players and developers of video games, or among players themselves. Some on-line video games needed transactions among players to be recorded, particularly to resolve conflict in the event of fraud. At the moment, this is done using databases distributed among players, relying on algorithms which have to achieve a balance between security on the one hand, and casual use and low cost for the hoster on the other. Solutions from the *blockchain* family could strengthen the first aspect, while not unduly slowing down the progress of the game.

Perhaps looking further ahead, *blockchain* could be used to record transactions among consumers on digitisable, cultural products, for instance, developing a secondhand e-book market, ensuring the same book is not both sold and retained by its first owner.

5.2.2. Blockchain for traceability

The literary and artistic property sector seems a natural home for use of *blockchain* to ensure traceability and authenticity of goods (digital or otherwise). Authorship issues for

a work, and authenticity problems, which are central to this sector, could benefit from the many advantages of this technology.

The initial description[19] of this usage certainly made the reader think about delivery of a manuscript. So it is entirely logical that the Ascribe start-up[20] is offering to track its customers' writings on the *blockchain*, so that they can subsequently claim attribution, as well as for distribution, as limited editions for instance.

Similarly in France, the Seezart[21] start-up intends to offer artists the opportunity to record authenticity certificates for their works on *blockchain,* once the pieces leave the workshop, to provide subsequent purchasers with additional guarantees of the provenance of the artwork. The *blockchain* will also allow the artwork to be tracked through its life, recording changes of ownership, or for instance, transfer to a restorer.

However, when several artists or participants (interpreter, producer, etc.) may claim rights over the same work, the question remains open of who is qualified to define and publish the sharing of these rights in the *blockchain*. As emphasised in the report from the University of Middlesex on music on *blockchain*[22], it will be essential to resolve the questions "who will enter the data?, about rights over a piece of music, and "how will these data be verified?".

Development of this practice also risks coming up against the difficulty of combining in one register all data relating to the rights over musical works, as the failure of the Global Repertoire Database in 2014 has shown.

5.2.3. Cultural smart contracts

Smart contracts are without doubt the most often quoted application of *blockchain* in the literary and artistic field, especially as regards automating the collection and payment of copyright and ancillary rights.

A start-up such as Ujo Music has the ambition to make the collective management bodies obsolete, or to replace them, by allowing musicians to collect the rights for their own works immediately they are played. So it could be imagined that in a disco, a device containing a microphone could record the music being broadcast, recognise the piece, identify the stakeholders in the *blockchain* and execute the contract by paying them the corresponding sum for the rights. While such an application could, in very simple cases (single artist, single consumer, set fee) require no intermediary, it is likely it would normally require third-party intervention, at any stage of the production of the piece of music (composer, interpreter, producer, etc.), for determining the division of rights, or to negotiate the fee for broadcast (fixed or as a percentage of turnover, etc.). The use of smart contracts could save time and improve transparency, but would certainly not lead to the disappearance of these intermediaries, whose usefulness lies first in being advisers and representatives, for stakeholders and artists, as well as having a fairly important role as promoters for consumers.

19 See part 3.2 of this report
20 https://ascribe.iohttps://www.ascribe.io/
21 http://www.seezart.comhttp://www.seezart.com

Another application of smart contracts in cultural industries, perhaps in the shorter term, could be facilitation of crowd funding, on the model of a DAO. An artist could thus request funding and offer automatic payment of "dividends" or copies of the work, through a smart contract.

5.3. The current and future potential of the various types of *blockchain* need to be better understood

Increasing enthusiasm for blockchain should not however be allowed to mask questions about the capabilities and conditions for implementation of the various platforms, now and in future. Even though the technical maturity stage has been reached, with some very relevant usages finding their place, it remains to be seen whether *blockchain*, as it develops over time, will be suitable for many other applications.

Every year, Gartner, the American consultancy firm specialising in new technology, publishes a "hype cycle", which classifies new technologies by their level of maturity, particularly in terms of identification of their most suitable applications. In 2017, *blockchain* was at the peak of "inflated expectations", which seems to point to some disappointments before it is implemented more widely. Gartner thus judged that it would be 5 to 10 years before *blockchain* reached its "plateau of productivity[23], the classic maturity period for this type of innovation.

Added to the uncertainties around the real potential of *blockchain* applications are the more philosophical conflicts remaining between the libertarian value system which oversaw its birth, and its appropriation by the very same major economic or institutional players which the original designers of this technology initially aimed to replace.

They reflect the ambivalence around *blockchain* at the moment, when it is hard to say whether it will upset the balance of the economic sectors in which it will be applied, encouraging the emergence of start-ups offering an innovative model based on this technology, or if it will, on the contrary, strengthen the existing players, through offering them efficiency and security gains. Either of these can be envisaged, at different times.

Finally, beyond these theoretical questions, we should also recall the practical issues which may arise if the reliable operation of many applications comes to rest on a few large *blockchains* (Bitcoin and Ethereum most often mentioned) whose stability, control and governance are still under discussion, and which will no doubt continue to evolve. The recent volatility of the Bitcoin currency[24], the concentration of processing capacity allowing the *blockchain* to be written in just a very few countries[25] and the problems in achieving consensus about the technical developments of the Bitcoin *blockchain* are just a few examples of this[26].

23 As an example, Gartner places the connected home and autonomous vehicles at the same level of "inflated expectation".
Quartz, 31 Dec 2016
The New York Times, 29 June 2016
Le Monde, 22 March 2016

6. Conclusion: *blockchain*, what are the challenges for public authorities?

On completion of this exploration of blockchain and its uses, the leaders of the mission would like to emphasise their initial sense that this technology, while bringing significant benefits to the sectors in which it will be applied, is presently only in the early stages of adoption, though developing fast. The reaction of established players has mainly been to adopt a proactive attitude, most often by developing pilot applications intended to gain greater understanding of how the technology works, proving the viability of particular usage concepts, identifying solutions for the contractual and regulatory problems raised, building new business relationships and learning to support these changes. Similarly, start-ups making *blockchain* their core value proposal are mainly in the early stages of developing their offering, and have hardly begun large-scale production.

However, the major changes which use of this technology may bring can only inspire the cultural world to become involved in it, and to develop its first projects, innovation being better than a wait-and-see policy for following (or even anticipating) constantly changing cultural practices.

Whether in the form of reports[27], experimental public practices or legislative responses aimed to assist private initiatives, governments in general have recognised the value of giving positive support to this emerging technology and its uses, without obstructing it too early by specific regulations.

However, this mission wishes to set out two main routes for the public authorities to respond in terms of the appropriation of *blockchain*.

The first involves the State as the regulator for the uses of *blockchain*. In addition to the recognition of the proof value offered by *blockchain*, potentially in legal terms, its increasing use will invite reflection on the definition of the rules of the game, whether in terms of consumer protection, for instance to identify the person responsible if a smart contract fails, or for setting the quality rules with which a *blockchain* must comply to be considered reliable for a particular use, to ensure court decisions are fulfilled in the *blockchain* or to apply legislation in this sector for respecting privacy or combating fraud (*know your customer*). Questions relating to the territorial scope of operations performed on the *blockchain* are also very likely to arise, as they do already for digital transactions.

27 See, in addition to the above-mentioned report from the State of Vermont, that from the United Kingdom Government Office for Science,

The second route brings the State in as a player for the *blockchain*. The first government applications of the *blockchain* which this report describes are themselves examples of the State as a user of the technology. No doubt the public authorities and their representatives will also be brought in as trusted third parties, directly or by appointment, whether to guarantee validity of the information entered in a *blockchain*, or to certify its reliability, on behalf of those who have neither the time or the knowledge needed to unravel the code. This increased security may also involve a reflection on opportunities for developing national or European "mining" capabilities, to avoid the situation where a single State concentrates in its own territory the computing power needed to change strategically important *blockchains*. Finally, and perhaps above all, the public authorities will be able to support private players in developing applications including blockchain, for instance by encouraging and even inspiring stakeholders to come together, and supporting the projects they bring.

Appendix 1: history of *blockchain* technology

Arrival in the media landscape

The *blockchain* technology was first conceived and described at the end of 2008, in an article published by Satoshi Nakamoto[28]. The purpose of this technology was to enable the rollout of an electronic currency, the bitcoin, while avoiding the need for a central authority to record and guarantee the reliability of the transactions. Emerging in the depths of the financial crisis, *blockchain* was thus designed originally, from a libertarian perspective, to allow financial transactions freed from the intervention of banks and central banks.

Aside from the development of bitcoin itself, between the first transaction using this currency in May 2010, and the point at the end of 2017 when the total value of bitcoins in circulation reached the equivalent of 200 billion dollars, *blockchain* mushroomed, arousing interest beyond its initial application, and gradually freeing itself from the sometimes negative image associated with "crypto-currencies".

The front page story about *blockchain* in the *The Economist* on 31 October 2015 no doubt helped awaken the general public's awareness of the possibilities this technology offered in many sectors.

The British weekly highlighted the main promise offered by *blockchain*: allowing people who did not trust each other to collaborate without needing a neutral, central authority.

Scientific relationships and breakthrough innovation from Satoshi Nakamoto

Virtual proto-currencies

The first work to give rise to virtual currencies (or crypto-currencies) dates back to the 1990s, with the research by Nick Szabo, for instance, on "bit gold", or that of David Chaum on "ecash". The common feature of these currencies is that they are created and transferred using encryption techniques, rather than through a central authority.

However, there were several technological obstacles to the development of these currencies. In 2008, the final technological obstacle left was the intangibility of the exchanges: when a piece of computer data is copied, the copy and the original are indistinguishable; so the very idea of a virtual currency seems compromised here: this is the "double spending" problem.

The whitepaper *from Satoshi Nakamoto and* bitcoin

The "*bitcoin whitepaper*" from Satoshi Nakamoto, published 2008, was the first realistic proposal to resolve this problem of "double spending", by introduction the concept of *blockchain*, which ensures the single use of a *bitcoin*.

The story of the "*bitcoin whitepaper*" is surrounded in mystery: the writer, Satoshi Nakamoto, is a pseudonym; it has never been claimed by any real person. The first publication was this "*bitcoin whitepaper"*. The quality of this first version, the low number of programming errors found subsequently, and the maturity of the engineering behind the bitcoin has even led to the idea it could be a group of people behind this avatar, rather than a single individual.

The first computer programme implementing the functionalities described in the "*bitcoin whitepaper*" was published in 2009, again by Satoshi Nakamoto. After a community formed around bitcoin which became sufficiently active to develop on its own, Satoshi Nakamoto transferred the programme's code to the bitcoin community, giving it the responsibility of developing and publishing updates to the virtual currency. He no longer appears after this.

While the essential idea developed by Satoshi Nakamoto was the creation of a currency, the technical solution offered has subsequently inspired numerous researchers and developers who have seen possibilities for use of this technology beyond that just of a currency.

Appendix 2: how does a *blockchain* work*?*

The first service a *blockchain* provides, that of allowing a user to take advantage of a digital resource, is made possible by a cryptography technique, asymmetrical encryption, already known for decades and used in contexts other than *blockchains*. The idea is to encrypt a virtual transaction (just a sequence of 0s and 1s) using a secret code, so that the transaction record can only be unlocked and used by the key-holder. A parallel in the physical world might be a (paper) ownership document placed in a transparent box closed with a padlock: anyone can see the document, but only the person with the key to the padlock can use the document.

Satoshi Nakamoto's main scientific and technical contribution was to have proposed a set of techniques offering the second service, that is, allowing users to transfer virtual securities with no central decision-making body involved.

Transaction transfers on a *blockchain* are split into blocks; each block is linked to the previous one (hence the term *blockchain*). Once the "current" block has completed the sequence of transfers, the participants in the *blockchain* system (the "miners") are invited to solve a cryptography puzzle depending on the block and on the solution to the cryptography puzzle of the previous block. The solution to this puzzle is entirely random, and is somewhat similar to a lottery: each participant has a chance of finding the solution first, in proportion to the power of their computer. The first miner to find the solution to the puzzle tells all the others; these check that the proposed solution is correct, they all accept the block, the transactions in this block are considered valid and a new block is created.

If a malicious miner wanted to modify a transaction from an old block, they would have to solve the cryptography puzzles of all subsequent blocks, since each puzzle depends both on the block with which it is linked and on the solution to the cryptography puzzle of the previous block, so that changing an old transaction invalidates all the cryptography puzzles after the block containing the transaction being modified.

Solving these puzzles by the miners provides the "proof of work" (POW) for the *blockchain* technology. Substantial computing power is needed to solve one of these puzzles, though it is not beyond the resources of one miner, but the computing power needed to resolve *all* the cryptography puzzles in one go is vast[29], so modification of a block already accepted (already "mined") is entirely unrealistic, if not actually impossible.

To encourage the miners to contribute to solving the cryptography puzzles and thus validate the blocks and transfer of transactions passing along a *blockchain*, the first miner to find a solution has the right to receive a reward, in the form of a transaction created for them.

29 In fact, the computing power needed adapts automatically, so that the difficulty of the cryptography puzzles to be resolved increases along with the total computing power of the miners on the *blockchain*.

Using this system, all users of a *blockchain* can agree about accepting a transfer of transactions, without having to use a central authority. Each user has one chance to mine the next block, and all the others can easily check that this mining is legitimate.

Finally, we should observe that there is no technical restriction placed on the participants of a *blockchain*. If anyone can "mine" the *blockchain*, it is said to be public, and it will be assumed that the many participants, each with various interests, do not have the option of coming to an agreement to subvert the *blockchain*, as the number involved guarantees its integrity. If on the other hand, a *blockchain* is only available to a small group of participants (and even if the transactions can be observed by anyone), this *blockchain* is said to be private (or of a consortium). In the latter case, the participants know each other beforehand, a governance structure may be in place, allowing conflict resolution among the participants, or else a central authority selected for the *blockchain*, for which the list of transactions and block it accepts will prevail, which takes such a use some way from the initial *blockchain* model.

Appendix 3: copy of the mission letter

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère Culture Communication

Paris, le 08 JUIL. 2016

Monsieur Jean-Pierre Dardayrol
Maître Jean Martin

Conseil supérieur de la propriété littéraire et artistique

182, rue Saint-Honoré
75033 Paris Cedex 01
France

Téléphone : 01 40 15 82 16
Télécopie : 01 40 15 88 45

cspla@culture.gouv.fr

http://www.culturecommunication.gouv.fr/Politiques-ministerielles/Propriete-litteraire-et-artistique/Conseil-superieur-de-la-propriete-litteraire-et-artistique

Monsieur, Maître, cher Jean-Pierre, cher Jean

Le succès des technologies de l'Internet a renforcé, dès le début des années 1990, l'intérêt pour les systèmes et les protocoles décentralisés, de la part des chercheurs, des entreprises puis des pouvoirs publics. Parallèlement, le succès du commerce en ligne a accompagné les progrès de la cryptographie. Dans ce contexte général, une novation parait particulièrement prometteuse, bien que parvenue aujourd'hui à des degrés différents de maturité et de complexité d'usage : les chaînes de blocs.

Les chaînes de blocs permettent de construire des bases de données décentralisées, sécurisées et historicisées d'événements. Elles présentent plusieurs avantages, du fait de cette décentralisation, de leur résilience et du faible coût des transactions. Elles présentent aussi des inconvénients, par exemple en termes de latence, d'interopérabilité ou de consommation d'énergie.

Le monde de la finance s'étant engagé activement dans leur appropriation, les chaînes de blocs ont permis depuis la fin des années 2000 l'éclosion de plateformes industrielles et d'environnements de développement, permettant de créer des applications variées, dont la plus emblématique concerne une crypto-monnaie. Des applications sont désormais en train d'apparaître dans l'univers des biens culturels, tant en Europe qu'aux États-Unis. Elles apparaissent comme prometteuses en raison des simplifications, de la sécurité et des baisses de coûts de transactions, notamment contractuels, qu'elles pourraient apporter.

Compte tenu de cet état de l'art, je souhaite que vous exploriez d'une part, l'état des lieux de cette technologie, et d'autre part, ses impacts potentiels sur la propriété littéraire et artistique. Il s'agira notamment d'évaluer ses apports pour la gestion des droits, l'accès aux œuvres ou encore l'optimisation des divers modes d'exploitation. Vous analyserez également les évolutions possibles en matière de contrôle de l'utilisation des

œuvres, dans un environnement de services distants dématérialisés et un cadre européen et internationalisé.

Je vous remercie vivement d'avoir accepté de prendre en charge cette mission, que vous pourrez conduire en vous entourant d'un comité de pilotage dont vous déterminerez la composition et en veillant à recueillir la diversité des analyses et expertises. Vous serez assistés en qualité de rapporteur par Monsieur Cyrille Beaufils, auditeur au Conseil d'État. Le cas échéant, vous pourrez vous adjoindre un second rapporteur. Vous établirez un rapport de mission pour le printemps de 2017, qui fera l'objet d'un premier rapport d'étape pour la fin de l'année.

Je vous remercie d'avoir accepté cette mission et vous prie de croire, Monsieur, Maître, à l'expression de mes sentiments distingués.

Et bien plus amicaux.

Le Président

Pierre-François Racine

Ministère de la culture et de la communication
Conseil supérieur de la propriété littéraire et artistique
(CSPLA)
182 rue Saint-Honoré
75033 Paris Cedex 01

Appendix 4: list of people and institutions examined (alphabetical order)

Association pour le commerce et les services en ligne (ACSEL)
- Eric Barbry, administrator, representative at CPSLA

Agence nationale de la sécurité des systèmes d'information (ANSSI)
- Côme Berbain, assistant deputy director for the expertise sub-division

Allmedia
- Pierre-Alexis Ciavaldini, co-founder

National assembly
- Lionel Tardy, deputy

Banque de France
- Thierry Bedoin, director of information systems organisation

Bensoussan avocats
- Eric Barbry

Blockchain France
- Alexandre Stachtchenko, co-founder
- Matthieu Riche, intern

Caisse des dépôts et consignations
- Philippe Dewost, deputy director, mission "Future investments programme"
- Nadia Filali, lead for "*blockchain*" programme

Crystalchain
- Sylvain Cariou, associate

Dailymotion
- Clément Reix, public affairs manager

École 42
- Françoix-Xavier Petit, director for innovation and partnerships

Editis
- Virgine Clayssen, lead for digital strategy

Fieldfisher
- Simon Polrot, lawyer

Hachette Livre
- Arnaud Robert, legal director

HADOPI
- Jean-Michel Linois-Linkovskis, secretary general
- Anna Butlen, general business director, head of legal affairs office

- Stephan Edelbroich, information systems director
- Didier Wang, engineer at the research and legal products division
- Olivia Bacin, lawyer

IDATE
- Yves Gassot, managing director
- Bertrand Copigneaux, senior consultant in innovation

Institut des hautes études sur la justice
- Antoine Garapon, secretary general

Ledger
- Nicolas Bacca, managing and technical director
- Vanessa Rabesandratana, communications director

Marçay - Bitoun lawyers
- Ismay Marçay, lawyer

Ministère de la Culture
- Nicolas Orsini, assistant head of digital innovation department
- Bertrand Sajus, mission leader at the digital innovation department

Open law
- Benjamin Jean, chairperson
- Camille Charles, mission leader

SACEM
- Jean-Noël Tronc, managing director
- Christophe Waignier, director for resources and strategy
- Charlotte Aïdan, legal officer for international affairs

SGDL
- Marie Sellier, chairperson
- , and Maïa Bensimon, legal officer

Seezart
- Jurgen Dsainbayonne, managing director
- Sandra Dsainbayonne, operations director
- Knuth Posern, technology director

Stormancer
- Jean-Michel Deruty, CEO

Télécom Paristech
- Patrick Waelbrock, professor of industrial economy and econometrics

Sessions

ADAGP
- “Traceability of the work of art or the power of its story”, 28 September 2017

AFNOR

- "New mechanisms for notarising transactions. How can "*Blockchain*" be standardised?", 17 October 2016

Conventions – Institut des hautes études sur la justice
- "*Blockchain*: what are the challenges for the world of law?", 15 December 2016

Conseil d'Etat
- "A-territoriality of law in the digital era". 28 September 2016

Seminar organised by the mission for the members of CSPLA

- Contributors:
  - Stéphane Bortzmeyer from AFNIC on the functional and technical aspects,
  - Patrick Waelbroeck, professor at Telecom ParisTech on the sectors of use and the ecosystem.
  - Christophe Waignier, SACEM, director of resources and strategy, on the use of *blockchain* to manage musical identifiers, around the world and by SACEM

- Participants
  - Debora Abramowicz, Procirep
  - Maia Bensimon, SGDL
  - Laurent Bérard-Quélin, FNPS
  - Léa Bernard, SNE
  - Boris Bizic, SNPS
  - Danielle Bourlange, APIE
  - Jean-Frank Cavanagh, GFII
  - Jean-François Debarnot, INA
  - Flore Grainger, SNE
  - Marie-Christine Leclerc-Senova, SCAM
  - Tania Lesaché, SNEP
  - Antoine Marie, ADAMI
  - Thierry Maillard, ADAGP
  - Benjamin Montels, USNAT
  - Gwenaêlle Masseron, CFC
  - Idzard van der Puyl, Procirep
  - Hubert Tilliet, SACD