Blockchain and intermediated securities

Hubert de Vauplane*

Abstract

Blockchain technology leads us to question the notions of possession and ownership. To what extent can information stored in a blockchain be considered a property right? Due to the global and distributed nature of the blockchain, how can conflict of laws issues be addressed? These issues can be illustrated in the context of intermediated securities law.

1. Introduction

Since its appearance a few years ago, the blockchain has been the subject of many legal studies.[1] Indeed, its technology raises particular legal questions. From the issues raised by *smart contracts*, to the protection of personal data, the blockchain has disrupted the traditional legal order by raising classic questions, but from a new angle. New because the characteristics of the blockchain force us to rethink the conventional legal order.

2. A brief overview of the blockchain

The blockchain is an *open source* protocol, with two characteristics. First, it is decentralised (it is intended to enable communication between machines without using a central machine). Second, it is consistent. This means that instead of having to consolidate information at a single point, which would be the central authority, all the information is available at each node of the network.[2] There is no more need for a central 'general ledger' to validate all the information. For example, in the case of bitcoin, all transactions are recorded after having been confirmed in each node of the network. It is therefore no longer necessary to have a central authority to ensure that there has been no fraud or double spending (i.e. use of the same bitcoin for two separate transactions). It is sufficient to check the consistency with all transactions or with

* Corporate Law Attorney, Kramer Levin LLP, Paris.

[1] The literature is wide and below is just a selection of it: T.I. Kiviat, 'Beyond bitcoin: issues in regulating blockchain transactions', *Duke Law Journal* (65) 2015, p. 570; P. Oudin, 'Decoding Blockchain Legal Issues – A Financial Law Perspective', November 2017, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3068189; M. Sherlook, 'Digital Securities', *Review of Banking & Financial Law* (35) 2015-2016, p. 586; A.W. & P. de Filippi, 'Decentralized blockchain and the rise of Lex cryptographia', 10 March 2015, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664; H. de Vaupane, 'La blockchain defiera-t-elle la règle?', *Revue de droit bancaire et financier* Nov.-Dec. 2016, p. 110.

[2] Each block in the chain contains the *hash* of the previous chain with the exception of the first block, also known as the genesis block (a *hash* is a mathematical operation that makes it possible to calculate a 'control' value from an original piece of data (file, string of characters, etc.), and the slightest change in this original piece of data will give a different *hash*). This ensures that the blocks follow each other in a chronological order. Indeed, it is impossible to generate the hash of block n without knowing the hash of block n-1. It is impossible to modify a previous block because this would affect all the following blocks. The mining activity consists in searching for a block n+1 in relation to the last block of the longest existing chain.

the previous node of the network. There are parallels between the Internet (TCP-IP) and the blockchain since they are both protocols allowing the creation of a decentralised infrastructure. Nevertheless, while the Internet transfers data packets from point A to point B, the blockchain allows 'trust' to be established between separate parties. In other words, with the blockchain, the 'trusted third party' becomes the system itself.

The blockchain technology emerged to solve a computer science problem, i.e. how to establish trust between two strangers who are members of the same network. This problem, known as the 'Byzantine generals' problem, consists of ensuring that a set of computer components work together to handle failures or malicious acts. The system must be able to maintain its reliability in the event that a minority of the components send erroneous or malicious information to circumvent the verification of double spending (fraud). To solve this problem, the protocol uses a cryptographic system based on a decentralised system of proof. Here, the proof of work requires a high computational capacity, provided by 'miners'. Miners are agents whose function is to supply the network with computing power, and to allow the updating of the decentralised database (list of transactions in the case of bitcoin). To update the database, miners must be able to confirm the new 'blocks' by decrypting the data (classic cryptography work). The more miners there are, the more difficult it is to assign the proof of work. Thus, the protocol can become virtually inviolable since the competition is strong at each node of the network, i.e. no group of miners becomes the majority.

To not be falsifiable, a blockchain[3] requires that no operator holds, at any time, more than half the computational power of the chain.

A blockchain is said to be public when everyone can read it and use it to perform transactions. It is also public when everyone can participate in the consensus-creating process. The most successful example of the public chain is Bitcoin. The governance of public chains, resulting from the *open source* movement and *cypherpunk*, is simple: '*Code is Law*'.[4] In this system, it is up to the nodes of the network to validate the choices debated and initiated by the developers by deciding to integrate or not the proposed changes. Its operation is based on 'cryptoeconomics', the combination of economic incentives and verification mechanisms using cryptography.

On the other hand, a blockchain is said to be private (or semi-private) when the consensus process can only be performed by a limited and predefined number of participants. Here, write access is issued by an organisation whereas read permissions may be public or restricted. The 'marketplace blockchains' between bankers or insurers are examples of private chains. In this case, the consensus process is controlled by a preselected set of nodes. Access to this blockchain may be public or limited to participants according to a process of co-optation.

The blockchain technology raises a series of classic legal questions whose analysis can be affected by its main characteristic, its operation in the form of a distributed network.

In the present article, I will only examine some aspects of securities law.

[3] Using a proof of work consensus method.

[4] L. Lessig, 'Code is Law', *Harvard Magazine*, January 2000, available at https://harvardmagazine.com/2000/01/code-is-law-html.

3. Ownership in the blockchain

If we take the case of the right of ownership, the question posed by the blockchain is to consider whether it is only a piece of evidence of a legal act or fact, or if it constitutes the legal act or fact itself. However, in many legal systems, the concept of ownership is closely linked to that of possession.[5] According to Ihering,[6] 'Possession is the objective realization of ownership'. It is the external realization of ownership. The owner is also the possessor of the asset, i.e. the good, or the right. Ownership is most often described by law as materialising a direct legal relationship between a good (a right) and a subject of law, while possession reflects a factual relationship between these same entities. In civil law systems, ownership is acquired in particular by possession, and possession proves ownership. In both cases, the regimes differ depending on whether it is moveable or immoveable property. Possession and ownership differ in their mode of acquisition. The transfer of possession is comparatively easier and less technical but the transfer of ownership in most cases involves a technical process of convincing. Possession is the exercise of *de facto* control over a good, regardless of whether or not this *de facto* control corresponds to a right. I possess such good because I hold it, because it is in my custody, I can physically touch it.

We can see the limits of this classic approach when it comes to the blockchain. First, it raises the question of whether the elements recorded in the blockchain constitute real rights or personal rights. Second, the approach is limited to the extent that its operating principle is based on a shared system of records. Regarding the question of the characterisation of the nature of the rights in the blockchain, at first glance, it seems difficult to see a real right (*right in rem*), i.e. a right *jus in re* insofar as the elements recorded in the blockchain are not physical goods but sequences of letters and numbers in the form of codes. However, these codes are both registered in a public key between the various stakeholders and in a private key, which is physical and held by only one person. As for the question of the functioning of the blockchain, the specificity is due to the fact that there is not a single register, but a multitude of registers shared between the actors. Therefore, the right, or the proof of the right, does not lie in a register but in all registers at the same time.

Here again, it is necessary to distinguish according to the role that one assigns to the 'distributed ledger', i.e. the multitude of registers. Although it is merely one piece of evidence of ownership, it differs from traditional registers by the fact that it is distributed, i.e. there are a multitude of registers all having the same 'probative value'. If these registers do not formalise ownership of a good or a right, but constitute ownership in themselves – in other words if the property right can only be exercised through the recording of the information in the blockchain – then a question arises of the relationship between this ownership and the possession. The good (or right), which is the subject of this ownership, is 'divided' over several registers. In fact, this first analysis should go a little further to see that in the blockchain, what is 'shared' is the public key; only this can be shared between several registers. However, the possession of a good (or a right) registered in the blockchain requires the combination of the public key and

[5] J.W. Salmond, *Jurisprudence*, 10th edn., London: Sweet & Maxwell 1947, p. 287; F. Pollock and R.S. Wright, *Possession in the Common Law*, Oxford: Clarendon Press 1888.

[6] J.M. Lightwood, *A Treatise on Possession of Land*, London: Stevens and sons 1894.

of a private key.[7] However, the private key remains in the possession of its holder, and is not distributed (or shared) between several blocks. This private key is a random number of 256 bits (32 bytes). There are 2 to the power of 256 possibilities of different private keys, i.e. 1.16 X 10 to the power of 77.

What holds the jurist's attention here is that the private key, to retain its entire security dimension, must only/can only be in the possession of its individual owner. If the private key is lost or stolen, the property registered in the blockchain (bitcoins or financial securities) is lost forever. There is thus a *de facto* relationship between the possession of the private key and the owner of the digital assets (bitcoins, or others) recorded in the blockchain. The possession of the private key is a physical, palpable, material element. The private key might be stored in a computer, on a USB medium, in a *wallet* or elsewhere, but it is 'somewhere'. There is no distribution in one or more registers of the private key, but it exists only in one place, one place which only its holder (owner?) can access. Thus, the right (of a claim or ownership) that constitutes a registration in the blockchain is divided in two, where each of the two parts is indispensable to the constitution of the right. One part is the public key, that is the internet network and its various servers. The other part is the private key, which is stored in a physical object. This right (whatever its nature) is somehow partially 'embedded' in a physical object and at the same time in the internet network. The importance of this point when analysing the field of conflict of laws will be discussed below.

4. What conflict of laws rules should apply for securities recorded in a blockchain?

The question of conflict of laws in a blockchain does not depend on the nature of the good or right that circulates or is recorded in the blockchain. However, given the fact that this question poses specific problems, I analyse the issues related to the conflict of laws in the blockchain for book-entry securities, so-called 'intermediated securities'.

The difficulties relating to conflict of laws issues in securities arise from the fact that it is difficult to determine the location of intermediated securities. Faced with a multiplicity of players, what book entry should be used to determine the rights of investors? Can the book entry with the issuer or its account-keeper be used, i.e. the law of the country where the securities are issued or those where they are held? Should the investor's book entry with one of the intermediaries be preferred and, in this case, which one? Should it be that of his own intermediary, that of the correspondent of this intermediary, or that of the depository or central custodian? All these questions have long been analysed and have found more or less satisfactory answers in the framework of the Hague Securities Convention[8] and various European directives and regulations. However, are these answers relevant when these same securities circulate, or are subject to transactions, via a blockchain?

[7] A. Mizrahi, 'A blockchain-based property ownership recording system', available at http://chromaway.com/papers/A-blockchain-based-property-registry.pdf.

[8] The Hague Convention of 5 July 2006 on the law applicable to certain rights in respect of securities held with an intermediary, available at https://www.hcch.net/fr/instruments/conventions/full-text/?cid=72.

5. Registration of securities within the blockchain

In the absence of an account on the blockchain, how can the transfer of ownership regime operate in it? The example of France is interesting here because, to my knowledge, it is the first case of domestic legislation on the rights attached to securities registered in a blockchain. An Order of 8 December 2017 defines the appropriate legal regime for the transfer of ownership of financial securities registered in a 'shared electronic recording device', i.e. a 'blockchain'. In fact, before this Order France had already introduced a legislative provision making it possible to use the blockchain technology for a particular type of debt securities, 'minibons'.[9]

The solution adopted by the French legislator to recognise the effects of a transfer of ownership of securities recorded in the blockchain lies in the establishment of a double legal fiction.

The first fiction consists in conferring on the registration of an issue or transfer of financial securities in a 'blockchain' the same effects as the book-entry of financial securities: 'Registration in a shared electronic recording device shall be considered a book-entry'.[10] The registration does not create a new obligation, nor does it reduce the existing guarantees relating to the representation and transmission of the securities concerned. This legal fiction was indispensable, to avoid having to create an entirely innovative legal regime. Indeed, we know that since the dematerialisation of securities in France in 1983, financial securities are only represented by a book-entry. In other words, it is the accounting aspect which determines the legal regime: it is because the securities are registered in a special account (which is called a securities account and which is subject to specific accounting rules) that a specific legal regime applies to them. This accounting approach is also decisive for ensuring the overall integrity since the concept of debit and credit and equivalence of positions between the issuing account with the issuer and the accounts opened in the name of the owners (with the issuer in the case of registered shares, or with the account holders in the case of bearer shares) ensures the security of the system. However, as we also know, there are no 'accounts' in the blockchain, but a sequence of information held in the form of a distributed register or ledger, without debit or credit. It is rather like the share transfer register for unlisted companies where transactions appear one after the other, in chronological order. Thus, whenever the concept of 'book entry' is mentioned in the Code, the Article in question is amended to be supplemented by the insertion of the concept of 'shared electronic recording device' already mentioned above. It is interesting to note that the legislator uses the verb 'to enter', which, attached to the concept of account, gave rise to the expression 'book entry' and will now allow its extension to that of 'register entry'. It is not certain that this choice of vocabulary is technically sound. In fact, the information contained in the blockchain is not 'entered' but recorded, insofar as this information appears in the form of computer codes.

The legal fiction means that this new method of registration of financial securities is an alternative to the book-entry and produces the same effects. The registration in a distributed register is not automatic (in contrast to the dematerialisation of securities in 1984) but requires a decision from the issuer. Of course, it will not be possible for the same issue to have securities

[9] The term 'shared electronic recording device' corresponds to the way in which the 'blockchain' technology, but more broadly the operation of distributed ledger technologies (DLTs), is already designated by the provisions of Art. L. 223-12 of the Monetary and Financial Code relating to minibons, introduced by Order no. 2016-520 of 28 April 2016 on savings certificates.

[10] Art. L. 211-3, para. 2 Monetary and Financial Code.

registered in an account and others entered in a register, insofar as there are no mechanisms to ensure the integrity of the issue.

This brings us to the second legal fiction. The reform does not change the nature of the right of the holder of the securities which depends on the form in which they are held: registration in an account or entry in a register. We know that French law establishes an equivalence between the registration in an account and ownership. Only the owner can be registered in an account.[11] Except in the case of a *nominee*. But can we still consider that the right of a holder of securities registered in a distributed register is a real right? This also appears to be a legal fiction, which consists of qualifying what is more akin to a personal right as a real right.

6. How is the current situation for intermediated securities affected?

As we know, blockchain technology or distributed ledger technology (DLT) can attribute an asset to a user without the need for intermediation. The 'thing' is represented by a unique piece of code and stored in an electronic vault that belongs to a participant of the chain. The value of this piece of code can be freely determined.

One of the main characteristic of the blockchain is the absence of an account: a blockchain is a block of information/transactions and these information/transactions are not recorded in an account in the meaning of debit and credit. Another characteristic of the blockchain is the absence of intermediaries or account providers. The concept of 'intermediated securities holding' as defined in the Hague Convention is challenged by the concept of DLT.

In a certain way, we can consider that securities 'held' within the blockchain are far removed from the intermediated securities holding system.[12] In the blockchain, legal relationships are not built on multi-tier relational rights beyond that account relationship but directly between participants of the chain. When, in the indirect holding system, there are no direct rights against the issuer or any intermediary other than an account holder's direct intermediary, the blockchain works as a direct system where investors have direct rights against the issuer. In this sense, the blockchain resembles the Nordic system[13] where investors have direct *vis-à-vis* with the issuer and intermediaries have no legal positions in securities recorded in the blockchain. However, there is one main difference from the Nordic system. In this system, there is only one legal ledger maintained in the central securities depository (CSD), whereas in the blockchain there are distributed ledgers without CSD.

[11] Art. L. 228-1, para. 6 of the Commercial Code.

[12] For a complete explanation of intermediated securities system and the differences with direct holding systems, see, Ch. Bernasconi, 'The law applicable to disposition of Securities held through indirect holding system', Hague Conference on Private International Law, prel. doc. no. 1, November 2000.

[13] In some of the Nordic countries, securities are in book entry form but each owner has an account to the CSD and can interact directly with the issuer. Read more: http://www.investorwords.com/15346/direct_holding_system.html#ixzz54kMt9IBf.

7. Toward digital Securities?

With the emergence of the blockchain, one wondered whether the legal nature of the securities registered in it was profoundly modified. Even to the point of speaking of 'digital securities',[14] which were also the subject of a registration with the Securities and Exchange Commission (SEC) in 2017.[15] In other words, has the legal relationship formed by the contract between the investor (shareholder or bondholder) and the issuer been altered by the decentralisation of the register? This is the debate that has shaken up the financial world in the search for a substantive law regime, not to mention a conflict of laws rule, on intermediated securities during the work on the Geneva Convention[16] and those on the Hague Securities Convention. Due to the presence of a chain of intermediaries (with the blockchain, there are no longer intermediaries, but a multiplicity of registers), is it still possible to consider that the law that governs the relationship between the holder of intermediated securities and the issuer can be qualified as a real property right? Would it not be appropriate, as US law has been able to do, to adapt the legal regime applicable to securities and stop resorting to a legal fiction to consider only the reality of the facts? Consequently, should the concept of right of ownership be abandoned and replaced with a right of claim of a specific nature? This debate has resurfaced with the emergence of the blockchain. How can one own securities entered in different registers all having the same legal 'value'? How is it possible to exercise possession (in the civil law meaning) over a digital asset? Is it not better to sweep away these fictions and only consider the securities registered in a blockchain as rights, and not goods? The debate is still moderate, due to the lack of conceptual analysis of this new regime. Substituting a real right by a personal right might seem to be the most logical solution at first. However, what kind of right are we talking about? If it is a right of claim, who is the debtor of this claim? The issuer, it would appear, but how is it possible to exercise a personal right via a blockchain? More fundamentally, will the holder of these securities be better protected through a personal right than with a real right? It is therefore necessary to reflect on a move toward a new form of *right in rem* on digital assets from a legal point of view, integrating the technological advances to build a specific legal regime that would allow the titular to get the possession of the title and the attributes of ownership on a digital asset. There are several precedents. The area of intellectual property, for example; this is a special legal regime which was created for intellectual works.

[14] M. Sherlock, 'Digital Securities: Overstock.com and Beyond', *Review of Banking & Financial Law* (35) 2015-1016, p. 586, available at https://www.bu.edu/rbfl/files/2016/10/Pages-from-Development-Articles-Formatted-10.pdf.

[15] P.L. Marcogliese and M.B. Rotter, 'Bitcoins and Blockchain – The Use of Distributed Ledger Technology for the Issuance of Digital Securities', available at https://www.clearymawatch.com/2016/01/bitcoins-and-blockchain-the-use-of-distributed-ledger-technology-for-the-issuance-of-digital-securities/.

[16] Unidroit Convention on Substantive Rules for Intermediated Securities (known as the Geneva Convention), 9 October 2009, available at https://www.unidroit.org/fr/instruments/marches-financiers/geneva-convention.

8. The conflict of law issue in the Blockchain

In the context of securities, harmonised conflict of laws rules can be found in several EU instruments:

- The Settlement Finality Directive[17] in relation to book entry securities provided as collateral to participants of settlement systems, the ECB or central banks from Member States;
- The Financial Collateral Directive[18] in relation to book entry securities provided under financial arrangements; and
- The Winding up directive concerning the enforcement of proprietary rights in book-entry securities in insolvency proceedings of credit institutions and investments firms.[19]

All three conflict of law rules are based on a similar approach: the PRIMA concept defined in the Hague Securities Convention, i.e. the Place of the Relevant Intermediary Approach. PRIMA departs from the traditional connecting factors referring to location or incorporation. Instead, it refers to the law of the securities account to which the relevant securities are credited. This law governs all securities credited to this account, whether foreign or domestic. The PRIMA model can be divided in two sub-models. The 'factual PRIMA', the law of the account is the law of the place where the account is factually (in practice) maintained. This subcategory is, more or less, the approach taken by the relevant EU legislation. The 'contractual PRIMA', the law of the account, is the law agreed upon to this effect by the parties in the custody agreement. This is the approach underlying the Hague Securities Convention, which is also the law in Switzerland and the United States.

The connecting factors in all three European directives differ in detail, but can be summarised as a register, an account, or a centralised deposit system. However, the concepts of 'register' or 'account' are not defined or are poorly defined in those directives. For instance, in the Financial Collateral Directive, register or account are the places where the 'entries are made'. These conflict of law rules do not specify where the account/register, centralised deposit system is 'located' or 'maintained'.

Here, we will consider the situation where the records in the chain are considered as the legal title, and not as a (mere) proof of evidence. Under the substantive law of some jurisdictions, the legal title of securities is identified with the recording in the blockchain. To achieve this situation, the applicable law must consider that the registration/recording in the blockchain is the legal title. This is the situation in France after the Order of 8 December 2017, which recognises the legal effect of securities recorded/registered with blockchain technology.

What could be the connecting factor when considering the nature of the right in securities as well as the conditions for enforceable acquisition and disposition of securities in a blockchain

[17] Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems, *OJ* 1998, L 166/45-50.

[18] Directive 2002/47/EC of the European Parliament and of the Council of 6 June 2002 on financial collateral arrangements, *OJ* 2002, L 168/43-50.

[19] Directive 2001/24/EC of the European Parliament and of the Council of 4 April 2001 on the reorganisation and winding up of credit institutions, *OJ* 2001, L 125/15-23.

system?[20] PRIMA presupposes the existence of accounts and therefore of intermediaries, which do not exist as such in the blockchain.

The first possible connecting factor is the entry point into the chain, i.e. the individual vault or wallet. Can we consider this as a connecting factor? It seems to be the more pragmatic answer and the more factual factor. Each transaction in the blockchain needs a vault, or wallet, where transactions are registered. However, this approach will not create legal certainty for third parties because there are as many entry points as there are participants in the chain.

The second possible connecting factor is the law of the issuer of the securities or *lex societatis*. This situation, however, will create significant legal uncertainty as the applicable law will be multiple in the case of an international portfolio of securities, i.e. securities issued by issuers located in more than one jurisdiction, in the electronic vault.

The third possible connecting factor is the law of the jurisdiction where the system (the blockchain) is located or supervised. This *lex systematis* appears to be similar to the Settlement Finality Directive.[21] However, although it should work for a private (or authorised) blockchain, it seems to have no sense in a public chain like Bitcoin or Ethereum.

The fourth option is the location of the private key. As seen above, any transaction in a blockchain needs a public and a private key. The private key is kept separately by the person entitled legal owner of securities. This option is tantamount to a *lex rei sitae*, as in the case of physical financial securities, since the place of custody of the private key will be considered the connecting factor to determine the law applicable to the transaction in the blockchain. The problem, of course, lies in the fact that third parties, but also the counterparty to the transaction, do not know this place of detention. In addition, because the private key is kept in the form of a USB key or in a laptop, this place can change at any time; this is the classic problem of mobility in private international law. There is therefore a great deal of legal uncertainty in this case. In the event of a discussion or dispute over the transaction, e.g. a sale, the applicable law will only be known by the seller of the securities who performed the transaction via his private key.

9. Conclusion

Recording securities in a blockchain opens new horizons, to the point of wondering whether all the debates of the 2000s on intermediated securities are now outdated. The challenges now lie in the establishment of a specific legal regime for these securities circulating in a blockchain. Given the blockchain's distributed nature, the absence of intermediaries and its global use, and easy to access to network, this immediately raises the question of the regulation of these transactions in a blockchain, and especially the conflict of laws in public chains (private blockchains generally have an applicable law and jurisdiction clause).

Regarding the conflict of laws rules, the criteria normally used in the area of securities are clearly inoperative. In fact, following the first basic approach set out above, I conclude that there is no immediately satisfactory answer to determine the connecting factor. Similarly, the matter of conflict of laws concerning securities circulating in the blockchain was studied in

[20] See Ph. Paech, 'Securities, intermediation and the blockchain: an inevitable choice between liquidity and legal certainty?', LSE, Society and Economy Working Papers 20/2015, update June 2016.

[21] Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems, *OJ* 1998, L 166/45-50.

the framework of the Expert Group established by the European Commission in 2017 on the conflict of laws regarding securities and claims.[22] However, the analysis was postponed to a later date given the intrinsic difficulty of the blockchain.

What can be concluded? Regarding securities circulating in the blockchain, there is no satisfactory answer to determine the law applicable to transactions. Accordingly, in the event that these transactions evolve and increase via a public blockchain, it becomes essential to define the legal regime of the ownership transfer of the securities sold in this in a separate deed blockchain.

[22] Available at http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3506.