Blockchain and Conflict of Laws[1]

Hubert de Vauplane
Avocat associé,
Kramer Levin LLP

Since its appearance a few years ago, the blockchain has been the subject of many legal studies. Indeed, its technology raises particular legal questions. From the question of the *smart contract*, 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.

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. The owner is also the possessor of the thing, 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 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 a given 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, because it raises the question of whether the elements recorded in the blockchain constitute real rights or personal rights, and then to the extent that its operating principle is based on a shared system of records. Regarding 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, we will see that these codes are both registered in a public key between the various stakeholders but also in a private key that it is physical, and which is held by only one person. As for the second point, namely the question of the blockchain's functioning again, the specificity is due to the fact that there is no single register, but a multitude of registers shared between the actors. Therefore, the right, or the proof of the right, does not lie in one register but in all registers at the same time.

Here again, it is necessary to be specific, in function of the role assigned to this distributed register. Although it is only one piece of evidence of ownership, it differs from traditional registers only by the fact that it is distributed, *i.e.* there are a multitude of registers all having the same "probative value". If this register does not formalise ownership but constitutes itself the ownership of a good or a right, in other words if the property right can only be exercised from the recording of the information in the blockchain, the question then arises as to the relationship between this ownership and the possession since 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 of a private key[2]. 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 sole owner. If the private key is lost or stolen, the property registered in the blockchain (bitcoins or financial securities) are 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. However, the possession of the private key is a physical, palpable, material element: this private key is stored in a computer, on a USB medium, in a *wallet* or elsewhere, but it is "somewhere". Otherwise, there is no distribution in a multitude of 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, it being noted that each of the two parts of this right is indispensable to constitute the right: on the one hand in the public key, that is to say in the internet network and its various servers; and on the other hand in the private key, which is 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 to continue the analysis in the field of conflict of laws will be discussed below.

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

The question of conflict of laws in a blockchain is a general question whose principles of analysis do not depend on the nature of the good or right that circulates or is recorded in

1 - This article derives from an article to be published to NIPR.

2 - Mizrahi, *A blockchain based property ownership recording system*, available at http://chromaway.com/papers/A-blockchain-based-property-registry.pdf.

the blockchain. However, given the fact that this question poses specific problems, we will 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 the 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: that of his own intermediary or 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 answers, more or less satisfactory, in the framework of the Hague Convention[3] and various European directives. However, are these answers relevant when these same securities circulate, or are even subject to transactions, *via* a blockchain?

How is the current situation for intermediated securities affected?

As we know, the Blockchain technology is able to 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.

Here, we will consider the situation where the records in the chain are considered as the legal title, and not as a proof of evidence. The legal title of securities is the recording in the blockchain. Of course, in order to achieve this situation, the law must consider that the registration / recording in the blockchain is the legal title. This is the situation in France after the Order of December 8, 2017 which recognises the legal effect of securities recorded / registered with blockchain technology.

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 "maintained" within the blockchain are far removed from the intermediated securities holding system. 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 intermediaries other than an account holder's direct intermediary, the blockchain works like a direct system where investors have direct rights against the issuer. In this sense, bockchain could be viewed as being similar to the Nordic system where investors have direct rights with the issuer and intermediaries take no legal positions in securities recorded in the blockchain. However, there is a main difference with the Nordic system: in this system, there is only one legal ledger maintained in the CSD, whereas in the blockchain there are distributed ledgers without CSD.

3 - The Hague Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary.

The Conflict of law issue in the Blockchain

Harmonised conflict of laws rules can be found in a number of EU instruments:

- Settlement Finality Directive in relation to book entry securities provided as collateral to participants of settlement systems, ECB or central bank from Member States;

- Financial Collateral Directive in relation to book entry securities provided under financial arrangements;

- Winding up directive concerning the enforcement of proprietary rights in book-entry securities in insolvency proceedings of credit institutions and investments firms.

All three conflicts of laws rules are based on a similar approach: the PRIMA concept defined in the Hague 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.

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 either 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".

What could be the connecting factor to consider the nature of the right as well as the conditions for enforceable acquisition and disposition in a blockchain system[4]? PRIMA presupposes the existence of accounts and therefore of intermediaries, which do not exist as such in the blockchain.

First possible connecting factor: the entry point to the chain, *i.e.* the vault or wallet. Can we consider this as a connecting factor? It seems to be the more pragmatic answer and factual factor: each transaction in the blockchain needs a vault, or wallet, where transactions are registered. However, this approach will not create legal certainty as there are as many entry points as participants in the chain.

Second possible connecting factor: the law of the issuer of the securities, the so called *lex societatis*. This situation, however, will create significant legal uncertainty as the applicable law will be multiple in the case of an international portfolio in the electronic vault.

Third possible connecting factor: the law of the jurisdiction where the system (the blockchain) is located or supervised. This *lex systematis* appears to be similar to the Settlement System Directive. However, although it should work for a

4 - See Ph. Paech, *Securities, intermediation and the blockchain : an inevitable choice between liquidity and legal certainty ?*, LSE, Society and Economy Working Papers 20/2015, up date June 2016.

private (or permissioned) blockchain, it seems to have no sense in a public chain like Bitcoin or Ethereum.

The fourth option would be the location of the private key. As discussed above, any transaction in blockchain needs a public and private key, and the private key is kept separately by the person who is entitled to be the 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 as 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, and that to the extent that 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 because in the event of a discussion or dispute over the transaction, the determination of the applicable law to deal with the validity and enforceability of the transaction will only be known by the seller of the securities who performed the transaction *via* his private key.

In fact, following this first basic approach, one realizes that there is no satisfactory answer to determine the connecting factor to the applicable law. It will be noted that the matter of conflict of laws concerning securities circulating in the blockchain was studied in the framework of the working group established by the European Commission in 2017 concerning the conflict of laws[5], but that 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, it is essential in the event of the development of these transactions *via* a public blockchain to define in a separate deed the legal regime of the transfer of ownership of the securities sold in this blockchain.

5 - http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3506.