Implications of the Blockchain Technology for the UNCITRAL Works

(Note: This version is subject to a final revision)

Koji Takahashi※

<Abstract>

The blockchain technology generates, via a chain of blocks, append-only ledgers which are distributed on online network and maintains them in sync with each other without the involvement of a trusted intermediary. It dispenses with a central registry and is capable of a myriad of applications.

The first half of this article examines what legal issues arising from the use of the blockchain technology may be resolved under the existing UNCITRAL works such as the Model Law on Electronic Commerce, the Model Law on Electronic Signatures, the Convention on the Use of Electronic Communications in International Contracts, the Model Law on Electronic Transferable Records, the Rotterdam Rules and the Model Law on Secured Transactions.

The second half of this article will examine the circumstances which raise the question whether it is possible to obtain the restitution of blockchain-based tokens by means of proprietary claims. Uncertainty over the availability of such claims is a problem of practical significance. It also calls for a globally unified solution but is untouched by the existing works of any international organisation. UNCITRAL, with its rich experience in the relevant areas, is an ideal and the natural forum for providing a solution to this problem.

<Table of Contents>

1. Overview...2

2. Under the Model Law on Electronic Commerce (1996) (EC Model Law), the Model Law on Electronic Signatures (2001) (ES Model Law) and the Convention on the Use of Electronic Communications in International Contracts (2005) (EC Convention)....................................3

3. Under the Model Law on Electronic Transferable Records (2017) (ETR Model Law) and the Rotterdam Rules (2008)..4

4. Under the Model Law on Secured Transactions (2016) (ST Model Law).........................7

a. Receivables denominated in a cryptocurrency 7

b. Units of cryptocurrencies... 8

c. Blockchain-based tokens representing negotiable documents.. 10

d. Blockchain-based tokens representing securities.. 11

※ Professor of Law at the Doshisha University Law School (Japan). I wish to record my gratitude to the UNCITRAL Secretariat for hosting me as a visiting scholar while I was undertaking research on the present topic. It greatly facilitated my understanding of the working of UNCITRAL.

e. Use of a blockchain-based distributed-ledger platform as a Registry for security rights...... 11
5. Proprietary restitution of blockchain-based tokens 12
a. Illustration of the problem.. 12
b. Legal bases of proprietary claims for restitution.. 14
c. Issues involved in the claims of different legal bases... 15
d. Why the problem calls for a globally unified solution 18
e. Approach to a uniform law making.. 20
6. Concluding remarks.. 22

1. Overview

The blockchain technology is an algorithm which was invented to create the Bitcoin cryptocurrency around 2009. Its significance lies in the fact that it has made it possible for a consensus to be reached (at a practical level) about the evolution of data on an open online network. It thus enables the synchronisation of distributed ledgers without the involvement of a trusted intermediary. For this reason, the blockchain technology is often called “the distributed ledger technology” and helps enhance the security and integrity of data. But the blockchain technology is not just about creating ledgers. It also makes it possible to trade tokens online on a P2P (peer-to-peer) basis and hold them without the involvement of intermediaries. The tokens are either cryptocurrency units of self-anchored value or asset-backed tokens, *i.e.* tokens for which there exists the underlying asset they represent. While the blockchain technology is capable of a myriad of applications, its potential is greatest in the areas where disintermediated P2P transactions can be made possible.

While the Bitcoin’s blockchain is public in the sense that it is a platform open to all who wishes to use it, there have also been many initiatives to create private blockchain platforms: either consortium type or fully private type. In common with public blockchains, they generate append-only distributed ledgers via a chain of blocks. However, unlike public blockchains, they are not open. Thus, consortium blockchains are a member-only platform where there exists an administrator who grants permissions to one group of members to make transactions and another (which may overlap with the former) to do the block validation. In common with public blockchains, however, they dispense with a central registry and operate instead with synchronised distributed ledgers. Accordingly, both public and consortium blockchains fall within the legal analysis of the present article, though which particular legal issues arise will depend on the precise configuration of the particular blockchain such as whether or not it is powered by tokens.[1] Fully private blockchains, on the other hand, merely

[1] Depending on the consensus algorithm adopted, a private blockchain does not require tokens of self-anchored value for incentivising the block validation. Even on such a blockchain, it is possible to issue

represent the replacement by the adopting organisation of its central database with distributed ledgers. Since it is a purely internal matter of the single organisation which adopts it, fully private blockchains do not fall within the present analysis except for the issue to be discussed at Ch. 4.e below.

In the first half of this article, we will examine the existing UNCITRAL works to see what legal issues arising from the use of the blockchain technology may be resolved under such works. In the second half, we will turn to examine a practically significant problem raised by the technology which calls for a globally unified solution but is untouched by the existing works of UNCITRAL or any other international organisation.

2. Under the Model Law on Electronic Commerce (1996) (EC Model Law), the Model Law on Electronic Signatures (2001) (ES Model Law) and the Convention on the Use of Electronic Communications in International Contracts (2005) (EC Convention)

One of the principles guiding UNCITRAL in its works in electronic commerce is the principle of technology neutrality or technological neutrality, which means that the law should neither require nor assume the use of a particular technology for communicating or storing information electronically.[2] The principle helps ensure that the law is able to accommodate future technological developments. Thus, the blockchain technology, though not yet invented when those three instruments were created, is not excluded from their scope of application.

It follows that under the EC Model law, admissibility in evidence or other legal effect may not be denied to information solely on the ground that it is in the form of a data message stored in a blockchain[3] (See Articles 5 and 9). In the context of contracts, an offer and the acceptance of an offer may be expressed by means of data messages stored on a blockchain (See Article 11, as affirmed by Article 8 of the EC Convention). The performance of contractual obligations are also subject to the EC Model Law and the EC Convention.[4] Article 12 of the EC Convention only mentions the formation of contract but States may, where appropriate under

and circulate asset-based tokens, *i.e.* tokens for which there exists the underlying asset they represent.

[2] See the Guide to Enactment of the Electronic Signatures Model Law (2001) para 5; the preamble of the Electronic Communications Convention. In the context of the EC Model law, the expression “media-neutral” is used to convey the same idea (See the Guide to Enactment of the Electronic Commerce Model Law (1996) para 24). Only later, has that expression come to be understood as referring more narrowly to non-discrimination between paper and electronic media (See the Guide to Enactment of the Electronic Signatures Model Law (2001) para 5).

[3] It is possible to embed metadata in, for example, the Bitcoin’s blockchain, which allows the extra information to be added to the Bitcoin transactions.

[4] Para. 81 of the Guide to Enactment of the Model Law; Article 1(1) of the Convention.

their legal systems, extend the principle by providing that the performance of a contract by an automated system may not be denied effect on the sole ground that no natural person intervened in each of the individual actions carried out by the automated system. This would improve clarity with respect to a so-called "smart contract."[5]

The principle of technological neutrality does not mean that any technology can create a data message which satisfies the paper-based requirements such as those of writing and a signature. Only the technology capable of fulfilling the purposes and functions of the paper-based requirements can create a data message which is deemed to meet those requirements. This is called the principle of functional equivalence, another principle underlying the UNCITRAL works in electronic commerce. Thus, the EC Model law sets out the conditions which a data message must meet to fulfill the purposes and functions of the paper-based requirements of writing and a signature (Articles 6 and 7). The ES Model Law elaborates on the conditions for the signature requirement. A data message stored in a blockchain will be deemed to meet the requirements of writing and a signature if it satisfies the respective conditions. The EC Model law also provides that there must exist a reliable assurance as to the integrity of information contained in a data message before the information is deemed to satisfy the paper-based requirement that it be presented in its original form (Article 8). The blockchain technology is particularly apt to provide a reliable assurance as to the integrity of information since it is tamper resistant.

3. Under the Model Law on Electronic Transferable Records (2017) (ETR Model Law) and the Rotterdam Rules (2008)

Whereas the three instruments examined above deal with data messages, the ETR Model Law deals with electronic transferable records (Article 1(1)). It sets out the conditions which must be met for an electronic record to be treated as a transferable document (Article 10). The latter is a document that entitles the holder to claim the performance of the obligation indicated in the document and to transfer the right to performance by means of the transfer of that document (Article 2). Bills of lading and warehouse receipts, for example, are covered. Electronic bills of lading are also covered by the Rotterdam Rules (United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea), which calls them "negotiable

[5] The expression "smart contract" is a misnomer. It is in fact a computer code stored on a blockchain, triggered by transactions on it and reads and writes data in it: Gideon Greenspan, "Beware the impossible smart contract" (2016) (http://www.multichain.com/blog/2016/04/beware-impossible-smart-contract/). The "smart contract" will give rise to a host of new legal issues but its relevance to a contract only lies in the fact that it can automate the online execution of the part of a contract which says "if A happens, then do B."

electronic transport records” (See Article 1(15)).

It should, however, be noted that the ETR Model Law is not applicable to cryptocurrencies such as the Bitcoin because a cryptocurrency holder has no right to claim any performance from anybody. Cryptocurrencies have self-anchored value because the participants in the underlying blockchain system are willing to accept them as a means of payment.

It should further be noted that an electronic equivalent of securities (such as shares and bonds) is outside the scope of the ETR Model Law (Article 1(3)). It follows that blockchain-based tokens representing securities (cryptosecurities) cannot be deemed to be securities under the ETR Model Law. A separate legislation would be needed to set out conditions for treating them as legally equivalents.

Both the ETR Model Law and the Rotterdam Rules adhere to the principle of technology neutrality. Thus, the draft explanatory notes for the ETR Model Law explain that reference in the Model Law to electronic transferable record management systems does not imply the existence of a system administrator or other form of centralized control.[6]

Both the ETR Model Law and the Rotterdam Rules also adhere to the principle of functional equivalence. They set out the conditions which electronic records must satisfy to fulfil the purposes and functions of the requirements relevant to transferable documents. Among such requirements, most important is the guarantee of singularity. Since a transferable document embodies the right to claim the performance of an obligation from another, it is essential to prevent multiple claims from being made on one and the same obligation. To this end, the law generally requires that there be only one original copy (or one set of original copies)[7] of a transferable document in circulation. In an electronic environment, providing an absolute guarantee of non-replicability may not be technically feasible since systems may retain copies of data. The ETR Model Law seeks to prevent multiple claims by requiring the use of a reliable method to identify an electronic record as the electronic transferable record and establish an exclusive control of it (Articles 10(1)(b)(i)(ii) and 11(1)(a)).[8] The Rotterdam Rules, too, treat the exclusive control of an electronic transport record as functionally equivalent to the possession of a transport document (Article 8(b)). Traditionally, the administrator of an electronic registry has been entrusted to ensure that the relevant electronic records are subject to the exclusive control of their holders. The blockchain technology is now capable of replacing such an administrator with an algorithm which guarantees that there is a single true version of distributed ledgers and ensures that the tokens recorded therein are subject to the exclusive control of their holders, *i.e.* the holders of the private keys.[9] There certainly are possibilities that

[6] Para. 167 of A/CN.9/920 (2017).

[7] It is an age-old practice to issue and circulate multiple copies of an original bill of lading.

[8] Para. 65 of the draft Explanatory Notes (A/CN.9/920 (2017)).

[9] For details, see Koji Takahashi, "Blockchain Technology and Electronic Bills of Lading" (2016) 22

a private key is disclosed intentionally or accidentally to two or more persons. More than one person would then have control over the cryptocurrency units held in the corresponding address. That would not, however, prevent the control from being characterised as exclusive since those persons have control to the exclusion of all others.[10]

The reliability of the above-mentioned methods will be assessed by adjudicators on an *ex post* (*i.e.* after the occurrence of a dispute) basis. It would, however, be unfortunate if there were no foreseeability as to which methods would pass the reliability test since the use of such methods would then be deterred. A thought should, therefore, be given to the possibility of compiling a list of reliable methods on an *ex ante* basis. Such a list would need to be reviewed from time to time because neither the configuration of a central registry nor the algorithm of a blockchain is permanently fixed.

The ETR Model Law also provides that the requirement of a signature may be met by an electronic transferable record only if a reliable method is used to identify that person (Article 9 on signature). The draft explanatory notes acknowledge that certain electronic transferable records management systems, such as those based on distributed ledgers, may identify a signatory by referring to a pseudonym rather than a real name.[11] The notes suggest that an identification by a pseudonym and the possibility of linking it to a real name, if need be, would satisfy the requirement to identify a signatory.[12] A remaining question is when it is sufficient to rely solely on a pseudonym and when it is necessary to have the possibility of linking a pseudonym to a real name. Signatures have a range of purposes.[13] To take signatures for endorsements as an example, where it is sufficient for signatures to establish that endorsements are back to back as under bills of lading, pseudonyms would be just as good as real names. Where, on the other hand, it is possible to make a recourse against endorsees as under bills of exchange or promissory notes,[14] it will be necessary to have the possibility of linking

Journal of International Maritime Law 202.

[10] The draft Explanatory Notes, *supra* note 8, also states at para. 95 that the reference to the person in control does not exclude the possibility of having more than one person exercising control.

[11] Para. 60 of A/CN.9/920 (2017). This interpretation is compatible with the understanding expressed in the Guide to Enactment for the Model Law on Electronic Signatures (2001) which states that the concept of identification may rely on other characteristics than a name (para. 117).

[12] Para. 60 of A/CN.9/920 (2017). The same interpretation may be given to the notion of "identification" of the person in exclusive control of an electronic transferable record, a requirement which must be met to establish functional equivalence to the possession of a transferable document (draft Article 11(1) on control).

[13] See the Guide to Enactment for the Model Law on Electronic Signatures (2001) para. 29.

[14] See Articles 15 and 77 of the Convention Providing a Uniform Law For Bills of Exchange and Promissory Notes (1930).

pseudonyms to real names. The explanatory notes further suggest that linking of a pseudonym to a real name may be based on factual elements to be found outside distributed ledger systems.[15] This stands to reason since sensitive information is not supposed to be stored on open ledgers.

4. Under the Model Law on Secured Transactions (2016) (ST Model Law)

Another existing work of the UNCITRAL which has relevance to the blockchain technology is the ST Model Law. Any asset having market value will generate demand for use as a collateral. In the light of the categorization of assets adopted by the ST Model Law, it will be convenient to classify blockchain-related assets into four groups: receivables denominated in a cryptocurrency, the units of cryptocurrencies, blockchain-based tokens representing negotiable documents, and blockchain-based tokens representing securities. After examining the creation and effects of security rights in those assets under the ST Model Law, we will turn our attention to the question whether a blockchain-based distributed-ledger platform may serve as a Registry within the meaning of the ST Model Law. The latter question can arise irrespective of whether the asset itself in which security rights are created is related to the blockchain.

a. Receivables denominated in a cryptocurrency[16]

The ST Model Law is applicable to security rights in “movable assets” (Article 1(1)). The words “movable asset” are defined broadly as a tangible or intangible asset, other than immovable property (Article 2(u)). Receivables are thus a “movable asset.” The ST Model Law contains a number of special rules for security rights in receivables (e.g. Article on contractual limitations on the creation of security rights; Articles 61 to 67 on the rights and obligations of third-party obligors). Such rules as well as the general rules contained in the ST Model Law would also be applicable to a receivable denominated in a cryptocurrency.

A right to payment of funds credited to a bank account is a receivable in the ordinary use of the word. But it is excluded from the definition of “receivable” under the ST Model Law (Article 2(dd)) as the latter contains a special set of rules for bank deposits (Article 25 on effectiveness against third parties and Article 47 on priority). If any bank should (by clearing regulatory hurdles) accept deposits in a cryptocurrency, those rules would be applicable to them. Are they also applicable to cryptocurrency units deposited with an online wallet provider? The answer depends on whether the provider falls within the expression “authorized deposit taking

[15] Para. 60 of A/CN.9/920 (2017).

[16] I wish to record my gratitude to Marek Dubovec for his helpful comments on this and next sections. Any remaining misconceptions are mine.

institution" within the meaning of Article 2(c) which defines the expression "bank account." If it is possible to give a broad and non-technical interpretation to those two expressions,[17] an online wallet provider may qualify to be an "authorized deposit taking institution" where it is authorized by law to receive the deposit of cryptocurrencies.

b. Units of cryptocurrencies

We are here concerned with the creation and effects under the ST Model Law of security rights in cryptocurrency units themselves rather than in a receivable denominated in a cryptocurrency. The practice of granting a consensual lien on cryptocurrency units already exists in financed purchases of them on an exchange.[18]

The ST Model Law provides that any type of movable asset may be encumbered (Article 8(a)) by a security agreement. Cryptocurrency units are a "movable asset," defined broadly by the ST Model Law as a tangible or intangible asset other than immovable property (Article 2(u)).

In order to create a security right under the ST Model Law, the grantor must have power to do so but does not have to be the owner of the encumbered asset (Article 6 (1)). Indeed, it will not be necessary for the asset to qualify for an object of ownership[19] since security rights need only to capture the value of the asset.

The encumbered asset must be described in the security agreement "in a manner that reasonably allows their identification" (Article 9(1)). This standard is met by a broad description which indicates that the encumbered assets consist of all the grantor's movable assets within a generic category (Article 9(2)).[20] It follows that a general description "all cryptocurrency" would suffice.

Where a security right is created in cryptocurrency units, the next question which arises is how to make it effective against third parties. One possibility is the registration of a

[17] The enacting State may alternatively wish to consider, as suggested by the draft Guide to Enactment of the Model Law (A/CN.9/WG.VI/WP.73, para. 39) as a possibility, replacing the term "authorized deposit-taking institution" with a generic term broad enough to include any institution authorized to receive deposits.

[18] See e.g. para. 3 of the terms of service of Bitfinex.com (https://www.bitfinex.com/terms).

[19] As examined *infra* at ch. 5.c, whether cryptocurrency units qualify for an object of ownership would currently be an open question under most legal systems.

[20] See also the UNCITRAL Legislative Guide on Secured Transactions (2007) chap. II, para. 58 (p. 79), which notes that many legal systems allow encumbered assets to be described in general terms, acknowledging that specific identification of individual items may not be practical or even possible for certain assets.

notice with respect to the security right in the Registry (Article 18(1)). Another possibility, the possession of the encumbered asset, is only available to tangible assets under the ST Model Law (Article 18(2)). The ST Model Law being merely a model for legislation, the enacting State may wish to make an exception for cryptocurrency units by equating the possession of a private key for cryptocurrency units to the possession of a tangible asset. The rationale for Article 18(2) is that the transfer of possession of the encumbered tangible asset eliminates the risk that third parties will be misled into thinking that the grantor holds unencumbered title to the asset.[21] The same risk may be avoided where encumbered cryptocurrency units have been transferred to an address for which the secured creditor possesses the private key.[22]

Under the ST Model Law, the word "money" is defined as currency authorized as legal tender by a State (Article 2(t)). A cryptocurrency would be capable of meeting this definition if any State authorized it as its legal tender.[23] However, "money" is supposed to be a tangible asset under the ST Model Law (See Article 2(ll)).[24] Consequently, the special rules for preserving negotiability of "money" contained in the ST Model Law (Article 48 on priority) are not applicable to cryptocurrencies. It follows that where cryptocurrency units are subject to a blanket security right covering all of the granter's movable assets[25] which has been made effective against third parties by registration,[26] the transferee would acquire them subject to the security right (See Article 34(1) on priority). This is so even if the transferee has no knowledge of the security right. It has been pointed out that a similar result arises under Article 9 of the U.S. Uniform Commercial Code, which has been considered problematic.[27] The ST Model Law would need to be amended if it is thought that cryptocurrencies ought to benefit from rules similar to those for money. In the meantime, the ST Model Law being merely a model, the enacting State may wish to devise special rules for cryptocurrency units to preserve their

[21] See *ibid.*, chap. III, para. 47 (p. 114).

[22] See *ibid.*, chap. I, paras. 80 and 81 (p. 50), where it is observed that in some States, control over intangible assets is treated as a notional possession of them since it achieves the ends comparable to those attained by the possession of tangible assets.

[23] One possibility is to authorise an existing cryptocurrency as a legal tender. There is also the idea of issuing the money of central bank on a blockchain ledger, which has been considered in a number of countries. The latter type of money should, however, be seen as receivables against the central bank denominated in a cryptocurrency and accordingly would fall within the foregoing analysis at Ch. 4.a.

[24] As seen above, a bank deposit is subject to another set of special rules.

[25] See Article 9(2).

[26] See Article 18(1) as well as the Model Registry Provisions Article 11(2).

[27] See e.g. Bob Lawless, "Is UCC Article 9 the Achilles Heel of Bitcoin?" (http://www.creditslips.org/creditslips/2014/03/is-ucc-article-9-the-achilles-heel-of-bitcoin.html) (2014); Jeanne Schroeder, "Bitcoin and the Uniform Commercial Code" (2015-2016) 24 U. Miami Bus. L. Rev. 1.

negotiability.

c. Blockchain-based tokens representing negotiable documents

The ST Model Law contains a set of special rules for "negotiable documents"[28] (e.g. Article 16 on creation, Article 26 on effectiveness against third parties, Article 49 on priority and Article 85(2) on the applicable law). But since "negotiable documents" are supposed to be a tangible asset under the ST Model Law (See Article 2(ll)),[29] electronic negotiable documents, including blockchain-based tokens representing negotiable documents, are not subject to the special rules for "negotiable documents." They instead fall within the concept of “intangible asset”, which is defined as “any movable asset other than a tangible asset” (Article 2(p)). But it is in practice pointless to create a security right in an electronic negotiable document unless it is extended, by virtue of the applicable law, to the tangible asset covered by the document (This indeed is what Article 16 does to “negotiable documents”, *i.e.* paper documents). Furthermore, as a result of the non-applicability of Article 49(3) (a provision for preserving the negotiability of “negotiable documents”[30]), a problem similar to that outlined above in the context of cryptocurrency units would arise with respect to electronic negotiable documents.

To avoid those problems, the enacting State may wish to extend the application of the special rules for “negotiable documents” to electronic negotiable documents. The adoption of the ETR Model Law would have the desired effect so far as the issues are covered by it.[31] This is because the ETR Model Law seeks to bridge the divide between the paper world and the electronic world by extending the application of paper-based rules to an electronic record which satisfies the requirements for functional equivalence to the corresponding "transferable document" as set out in Article 10 of the ETR Model Law (hereafter "qualifying electronic transferable record"). It should be noted that, as examined above, a blockchain-based token, too, can be a qualifying electronic transferable record. It should also be noted that the notion of "transferable documents" under the ETR Model Law largely overlaps with that of "negotiable

[28] The Model Law contains no definition of this term. According to the Legislative Guide on Secured Transactions, Introduction, para. 20 (p. 10), it means a document, such as a warehouse receipt or a bill of lading, that embodies a right to delivery of tangible assets and satisfies the requirements for negotiability under the law governing negotiable documents.

[29] The Legislative Guide on Secured Transactions, too, was prepared against the background of paper-form negotiable documents (*ibid*., p. 11 at fn. 25).

[30] See *ibid*., ch. V, para. 167 (p. 228).

[31] The Guide to Enactment of the Model Law on Secured Transactions, at para. ***????***, suggests that States adopting both model laws should consider their relationships, leaving the States to make their own analysis.

documents" under the ST Model Law. It follows that a security interest created in a qualifying electronic transferable record would be extended to the tangible asset covered by it by virtue of Article 16 of the ST Model Law. The requirement of “possession” of a “negotiable document” under Articles 26, 49 and 85(2) under the ST Model Law would be met by the “exclusive control” (Article 11 of the ETR Model Law) of a qualifying electronic transferable record. Consequently, Article 49(3) (the provision for preserving the negotiability of “negotiable documents”) would also be applicable to a qualifying electronic transferable record under "exclusive control," which avoids the problem identified above. But the determination of “the State in which the document is located” under Article 85(2) is not assisted by the ETR Model Law since the latter contains no provision for determining the place in which an electronic negotiable document is deemed to be located.

d. Blockchain-based tokens representing securities

Under the ST Model Law, “non-intermediated securities” are securities (*i.e.* shares and bonds)[32] other than those credited to a securities account (Article 2(w)). “Securities account” is in turn defined as meaning an account maintained by an intermediary to which securities may be credited or debited (Article 2(ii)). A blockchain would make it possible to trade securities on a P2P basis and hold them without the involvement of a trusted intermediary. Blockchain-based tokens representing securities (cryptosecurities) would, therefore, be “non-intermediated securities.” They are also unrepresented by a “certificate”, which under the ST Model Law refers only to a tangible document subject to physical possession.[33] It follows that cryptosecurities would fall within the definition of “uncertificated non-intermediated securities” (Article 2 (mm)). They would accordingly be subject to special rules for such securities as contained in the ST Model Law (Article 27 on effectiveness against third parties and Article 51 on priority). Thus, a security right in cryptosecurities is made effective against third parties by the conclusion of a control agreement (between the grantor, the secured creditor and the issuer) (See Article 27) and has priority over a security right in the same cryptosecurities for which registration is made in the Registry (See Article 51(3)).

e. Use of a blockchain-based distributed-ledger platform as a Registry for security rights

Under the ST Model Law, the registration of a notice in the Registry renders the security right effective against third parties (Article 18(1)). Can a distributed-ledger platform serve as a Registry?

[32] See para. 54 of the draft Guide to Enactment (A/CN.9/WG.VI/WP.73).

[33] *Ibid.*, para. 40.

The ST Model Law contains in Chapter IV a set of rules called "Model Registry Provisions." Those rules envisage the existence of a registrar who administers the Registry (Article 27). Public blockchains are not administered by any specific person and accordingly would not fit this profile. The administrator of a private blockchain may, on the other hand, be appointed by the enacting State to be a registrar under Article 27. Through the power of appointment and dismissal, the enacting State is ultimately in charge of the Registry's operation. It would in fact be unlikely for any State to put faith in public blockchains since they are not controlled by any specific entity. Besides, the consensus algorithm of a public blockchain which relies on the "longest chain rule" is incompatible with the provisions in Article 13. The former leaves the possibility that in the event of a fork, records in a chain will be abandoned in favour of those in another chain which eventually becomes longer. The latter, on the other hand, makes the registration of a notice effective when the information in the notice is entered into the Registry record and provides that the information must be entered in the order in which each notice is submitted. With a private blockchain, it should be possible to devise a consensus algorithm compatible with the provisions in Article 13. Furthermore, blockchain ledgers, which are an append-only log, are perfect to fulfill the requirement that the Registry must preserve all information contained in the record (Article 29(2)). It follows that distributed ledgers on a private blockchain platform may serve as a Registry.

5. Proprietary restitution of blockchain-based tokens

Having examined the existing works of UNCITRAL, we will now turn our attention to a problem which is untouched by UNCITRAL or any other international organisations. There are a number of circumstances which raise the question whether it is possible to obtain the restitution of blockchain-based tokens by means of proprietary claims. Among the private-law issues arising from the use of the blockchain technology, uncertainty over the availability of such claims seems to be a problem of particular significance. It also calls for a globally unified solution.

What follows will illustrate the problem, outline the legal bases of claims which may be made, and identify the issues involved in such claims. It will then explain why the problem calls for a globally unified solution and consider what approach should be taken to make a uniform law.

a. Illustration of the problem

The pre-existing forms of electronic money, which are often in the shape of pre-paid cards, provide the holders with credits redeemable from the issuers. Accordingly, most legal problems may be handled under the law of obligations. By contrast, holding cryptocurrency does not by itself entitle the holder to any claim against anybody. Accordingly, proprietary issues become more important.

The significance of proprietary issues is most evident where insolvency hits the holder of cryptocurrency units who, in a variety of circumstances, is under obligation to return the units to another person. That other person may join other creditors in the insolvency proceedings, which would usually yield to him only a partial recovery. But if he could make a proprietary claim to obtain the restitution of the units, he would be able to make a full recovery.[34] The availability of such a claim is, however, currently unclear. The problem arises in a number of circumstances such as those described in Cases 1 to 3 below.

Case 1: Theft of cryptocurrency units.
Suppose that cryptocurrency units have been stolen by means of, for example, malware and then transferred to third parties. The original holder may have a claim in tort for damages covering the value of the stolen units against the thief or against a *mala fide* transferee. But it would not lead to a full recovery in the case of insolvency of the thief or transferee. If the original holder has a proprietary claim for the restitution of the units, he will be able to obtain a full recovery.

Case 2: Mistaken remittance of cryptocurrency units.
Suppose that cryptocurrency units have been mistakenly remitted to a wrong address or in a wrong quantity. The sender may have a personal claim against the recipient in unjust enrichment for the restitution of the value of the units. But it would not lead to a full recovery if the recipient has become insolvent. If the sender has a proprietary claim for the restitution of the units, he will be able to obtain a full recovery.

Case 3: Entrusting of cryptocurrency units to another person.
While the blockchain technology allows cryptocurrency units to be held and traded without the involvement of intermediaries, the users may opt to entrust ancillary service providers with their cryptocurrency units for reasons of convenience. Thus, instead of holding their cryptocurrency units themselves, some may use an online wallet, entrusting their units to the wallet provider. Again, many users of cryptocurrencies buy and sell them through an online exchange and in the course of transactions entrust the exchange provider with their cryptocurrency units. These customers would have a contractual claim for the return of their cryptocurrency units or their value from the provider of wallet or exchange. But it would not lead to a full recovery if the provider becomes insolvent. If the customer has a proprietary claim for the restitution of the units, he will be able to obtain a full recovery.

[34] It should be noted that for creditors who have no proprietary claim for restitution, there remains the possibility of obtaining priority over other creditors conferred by a statutory lien.

There is a real case in point. Mt.Gox was once the world's biggest provider of a Bitcoin exchange. It became insolvent and entered into winding-up proceedings. Most of the creditors were its former customers who had entrusted it with bitcoins and/or fiat currencies. One of them filed a suit against the insolvency representative, seeking a full recovery of the bitcoin units of which, or the value of which, he had a contractual right to return from Mt.Gox. He did so by asserting ownership over them rather than making a personal contractual claim.[35]

The proprietary issues also have practical significance outside the context of insolvency. Thus, if cryptocurrency units have been seized by a creditor of the holder, the person who has a proprietary claim for the restitution of the units would be able to challenge the seizure. Such situations can also arise from a number of circumstances including those described in Cases 1 to 3 above.

The significance of the proprietary issues extends beyond cryptocurrencies to non-monetary tokens which may be traded and held on a blockchain, such as those representing securities (cryptosecurities),[36] those for controlling domain names and those used in an ICO (Initial Coin Offering).[37] Circumstances analogous to those described in Cases 1 to 3 above will raise the question whether it is possible to obtain their restitution by means of proprietary claims.

b. Legal bases of proprietary claims for restitution

A proprietary restitutionary claim may most obviously be based on ownership. The legal systems which have inherited the Roman law concept of ownership, *dominium*, would allow an action to be filed for *rei vindicatio* (vindication of property: an owner's claim against the possessor for the return of the property)[38] which may be made outside insolvency proceedings. The plaintiff's claim in the Mt.Gox case outlined above falls within this category.

For other legal systems, notably common law systems, *rei vindicatio* is an alien concept. Thus, in the English common law, the tort of conversion fills the gap of the missing *vindicatio*. Although nominally tortious, it has become the remedy to protect the ownership of

[35] For the outcome of the case, see *infra* ch. 5.c.

[36] See e.g. Philipp Paech, "Securities, intermediation and the blockchain: an inevitable choice between liquidity and legal certainty?" (2016) 21(4) Unif Law Rev 612, 637.

[37] It is a means of raising capital which IT start-ups have begun to use. They issue and sell coins (tokens) on a blockchain which entitle the holders to receive services and dividends from them. Besides the private-law issues examined by this article, this method raises regulatory issues: See e.g. the U.S. Securities and Exchange Commission, "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO" (Release No. 81207 / July 25, 2017).

[38] e.g. section 985 of the German BGB (Civil Code).

goods.[39] The delivery of the goods may be ordered at the discretion of the court,[40] which will be exercised where the defendant is insolvent.[41]

In some legal systems, a proprietary restitutionary claim may alternatively be made on the basis of a resulting or constructive trust. Where the claimant can show that he has an equitable proprietary interest in property that is in the possession of the defendant, the court may declare that the property is held on trust for the claimant and it will order the defendant to transfer this property in specie to the claimant.[42] Many claims to a resulting or constructive trust are motivated by the principle that property held by the bankrupt on trust for another person does not form part of the bankrupt's estate.[43] Thus, in Re Goldcorp Exchange Ltd,[44] a dealer in gold became insolvent and its customers sought a declaration that the dealer had held bullion on trust for them. In another case, Chase Manhattan v. Israel-British Bank,[45] a transfer of a dollar-denominated bank deposit was made in error and the transferee was subsequently would up. The transferor sought a declaration that the transferee had become a trustee of the paid sum for the transferor. It can be anticipated that a claim to a resulting or constructive trust will be triggered to obtain the restitution of blockchain-based tokens in such circumstances as those described in Cases 1 to 3 above.

c. Issues involved in the claims of different legal bases

Where an ownership-based *vindicatio* claim is made to seek the restitution of blockchain-based tokens, the first issue which must be addressed is whether such tokens qualify to be an object of ownership. Thus, in the Mt.Gox case outlined above, the Tokyo District Court dismissed the claim by denying that bitcoin units could be an object of ownership.[46] The court's reasoning rested on a formal analysis as it relied on the Japanese law concept of "*shoyûken*," a concept which signifies ownership but is statutorily limited to tangibles as its objects. Some legal systems, like Japanese law, restrict the object of ownership to tangibles while others extend it to

[39] OBG Ltd v Allan [2007] UKHL 21, para. 308 (House of Lords). See also Andrew Burrows (*ed.*) *English Private Law* (3rd ed., 2013) paras. 17.304 and 17.309 [Donal Nolan and John Davies].

[40] Torts (Interference with Goods) Act 1977, s 3.

[41] See Richard Calnan, *Proprietary Rights and Insolvency* (2nd ed., 2016) para. 2.108.

[42] See e.g. Boscawen v Bajwa [1996] 1 WLR 328, 335 (English Court of Appeal); Giumelli v Giumelli (1999) 196 CLR 101 [3] (High Court of Australia).

[43] Andrew Burrows (*ed.*) *English Private Law* (3rd ed., 2013) para. 4.152 [William Swadling].

[44] [1995] 1 AC 74 (Privy Council).

[45] [1981] Ch 105 (English High Court).

[46] The judgment of the Tokyo District Court on 5 August 2015 (2015WLJPCA08058001).

intangibles.[47] In the systems which belong to the latter camp, the exact category of intangibles which qualify as an object of ownership may not be set in stone. In the legal systems which currently restricts the object of ownership to tangibles, whether the law should remain static is another question. The blockchain-based tokens may compel the legislature and judiciary in each State to consider *de lege ferenda* (with a view to the future law) whether their concept of ownership should embrace them.[48] A case may be made for treating certain kinds of them as being an object of ownership by distinguishing them from other digital assets or data on account of, *inter alia*, their amenability to exclusive control by the holders.[49]

The same issue will arise where the restitution of blockchain-based tokens is claimed in tort of conversion.[50] It has been litigated whether the remedy of conversion is available to protect intangibles such as choses in action,[51] information in a database[52] and domain names.[53] The blockchain-based tokens will be a latest addition to this list.

If blockchain-based tokens, or certain kinds of them, qualify to be an object of ownership, the next question to be addressed is what should be the test for determining the owner. It would accord with the intuition of many users of such tokens to consider that the holder of the private key for the address at which tokens are held owns them. This intuition

[47] Akkermans classifies German and Dutch laws into the former category, while French law in the latter (Bram Akkermans "Property Law" in Jaap Hage & Bram Akkermans (ed.) *Introduction to Law* (2014) 71, 78). Von Bar and Drobnig add Greek law to the former camp and the laws of Portugal, Italy, Austria, Belgium, Spain, Sweden, and Scotland to the latter (Christian von Bar and Ulrich Drobnig, *The Interaction of Contract Law and Tort and Property Law in Europe A Comparative Study* (2004) 317).

[48] For academic discussions, see e.g. Shawn Bayern, "Dynamic Common Law and Technological Change: The Classification of Bitcoin" 71 Wash & Lee L Rev Online (2014) 22, 34; Joshua Fairfield, "BitProperty" 88 S. Cal. L. Rev. 805 (2015); David Quest, "Taking security over bitcoins and other virtual currency" (2015) 7 JIBFL 401; Matthew Lavy & Daniel Khoo, "Who Owns Blockchains? An English Legal Analysis" (http://sclbc.zehuti.co.uk/site.aspx?i=ed47875 (2016).

[49] It should be noted by way of contrast that the digital assets of an online game disappear if the provider of the game erases the data on its server.

[50] Sjef van Erp, "Comparative Property Law" in Mathias Reimann & Reinhard Zimmermann (*eds*), *Oxford Handbook of Comparative Law* (2006) 1044 at 1062, notes that what qualifies as an object of property law is a fundamental property law question which is as pressing in the civil law systems as in the common law systems. The author cites domain names, the right to use a wireless network and emissions quota as examples of possible new objects.

[51] OBG v Allan [2007] UKHL 21 (House of Lords).

[52] Your Response Limited [2014] EWCA Civ 281 (English Court of Appeal).

[53] Kremen v Cohen, 337 F 3d 1024 (2003) (U.S. Court of Appeals for the Ninth Circuit).

presumably stems from the fact that the holder of the private key has an exclusive control over the tokens. But the rule cannot be as simple. For one thing, there are situations which require an elaboration of what it means to be the holder of a private key as where the private key has been intentionally or accidentally disclosed to two or more persons. For another, there may be circumstances in which it is thought that an ownership-based claim for the restitution of tokens should be allowed against the present holder. Each of the circumstances described in Cases 1 to 3 above merits consideration in this light. Thus, the case for allowing such a claim may be considered to be stronger where the holder is a thief (Case 1) or an online wallet provider (Case 3) than in other situations. Such circumstances as described by Cases 1 and 2 would also raise the questions whether the *nemo dat* rule (that no one can give a better title than he himself has) should prevail and when exceptions, if any, should be made.[54]

Where a proprietary claim arising from a resulting or constructive trust is made to seek the restitution of blockchain-based tokens, it is not necessary to consider whether such tokens can be an object of ownership in the sense of a source of *vindiatio* claim. Intangible assets are capable of being trust property[55] and so will be blockchain-based tokens. But another issue, no less difficult, will arise: under what circumstances the holder of blockchain-based tokens is deemed to hold them on trust for the claimant.

Whether the claim for restitution is based on ownership or arises from a resulting or constructive trust, it gives rise to the additional question, namely in what way the tokens must be identified. If specific identification were required, it would have to be possible to technically trace the tokens of which restitution is sought. The transactions of blockchain-based tokens are traceable since they are recorded immutably in the blockchain. This should make the task of identification of blockchain-based tokens easier than would be the case with tangible goods. It should, however, be noted that while transactions are traceable on a blockchain, tokens are less so unless they are individually coloured. Consequently, it will often be difficult to specifically identify the tokens of which restitution is sought. It is important, however, to realise that what matters in law is not technical traceability but normative traceability. To affirm normative traceability, it may be enough to be able to say that the person from whom the restitution is sought could be deemed to hold all or part of the units of which the restitution is sought. To illustrate the point by an easy case, suppose that Alice had 70 units at her address. Bob has stolen them through a phishing attack and transferred them to his address in which they have been mixed up with the 30 units he had held there. Unless the stolen 70 units had been coloured,

[54] For a consideration under English law, see Joanna Perkins and Jennifer Enwezor, "The legal aspect of virtual currencies" [2016] 10 JIBFL 569.

[55] With respect to an emissions quota, see Armstrong DLW GmbH v Winnington Networks Ltd [2012] EWHC 10. More generally, equitable property interests can be created over assets which the common law does not regard as property: See Calnan, *supra* note 41, para. 2.69.

it will not be technically possible to say which of the 100 units Bob now holds at his address are originally Alice's. It is, however, possible to say that Bob holds the stolen 70 units. The question will certainly become more difficult if Bob makes a transfer from his address. But it may be possible to normatively trace the stolen units up to some point.

d. Why the problem calls for a globally unified solution

If each national legal system is left to its own device, divergent positions may emerge over each of the issues examined above. Thus, legal systems may come to differ as to whether blockchain-based tokens qualify as an object of ownership and what are the tests for determining owners. Although legal uncertainty arising from divergence among national laws may be mitigated if the governing law is predictable, it is not clear for reasons examined below what law governs proprietary claims for the restitution of tokens on a public blockchain. The lack of clarity and predictability of governing law, coupled with the novelty and practical significance of the problem, makes a strong case for a globally unified solution.

New issues of contract law, by contrast, do not immediately call for a globally unified solution. Rather, there is a lot to be said for leaving them to be dealt with by each domestic law for the time being. This is because party autonomy is well established as a principle of choice of law for contractual issues.[56] It allows contracting parties to choose the legal systems which they find will provide the best rules for their contract. This provides legal certainty for the parties and may at the same time motivate the national law makers to compete with each other with a view to making their legal system attractive for parties' choice. When favoured rules eventually emerge, an international unification may then be attempted along such rules.

For proprietary issues, party autonomy is generally not accepted as a choice-of-law principle. In the first place, it is unworkable between the parties whose relationships are not contractual except to the extent *ex post* (after the event) choice is permitted. Furthermore, the freedom of parties to choose the governing law by agreement can produce the fragmentation of governing law among different pairs of parties. Such a result might not be seen so unpalatable in the eyes of some legal systems, typically common law systems, which handle proprietary questions relatively, namely by asking which of the two competing litigants has the better right. On the other hand, the legal systems which have inherited the Roman law concept of ownership, *dominium*, would favour the absolute exclusivity, or the *erga omnes* ("towards everyone") effect, of ownership. It is true that this conceptual absoluteness tolerates some relativism to

[56] As reflected in Article 2 of the Hague Principles on Choice of Law in International Commercial Contracts, a text which has been endorsed by UNCITRAL (Report of the 48th session (2015) A/70/17 para. 240).

creep in at the evidential level due to difficulties of proof:[57] since the perfect proof of ownership tracing up all prior transactions to the first owner would be difficult or impossible, it is described as a devil's proof ("*probatio diabolica*"). At the choice-of-law level, however, it makes more sense to specify a single law for determining ownership irrespective of who, among a number of stakeholders, are the litigants in a particular case.

With respect to tangible goods, it is well established that proprietary issues are governed by the law of the country where it is situated (*lex situs*). With respect to intangibles, of which blockchain-based tokens are an example, choice-of-law rules are far from settled. With respect to an emissions quota, which is financially valuable data like a blockchain-based token, it has been suggested that the proprietary issues should be subject to the law of the country where it is registered.[58] This connecting factor does not work with a blockchain-based token since it is not registered on a national registry. Where a consortium blockchain is used, it may be possible to ascertain the law of the country with which it is most closely connected by having regard to the country in which it is administered. On the other hand, a public blockchain is not administered by any specific entity and the tokens are recorded on ledgers which are distributed on a borderless network. This makes it difficult to localize tokens on a public blockchain and consequently renders the governing law of their ownership unclear.

The same problem of uncertainty exists where a restitutionary claim is made for the tort of conversion. It has been suggested that the claim should be characterized as proprietary for choice-of-law purposes since, although it is nominally tortious, property rights are ultimately at stake.[59] As seen above, this characterization does not lead to clear choice-of-law rules where tokens on a public blockchain are the object of the claim.

The governing law of a proprietary restitutionary claim arising from a resulting or constructive trust is no clearer. Some have argued that it should be specified by the choice-of-law rules for unjust enrichment[60] on the ground that constructive trusts arise in response to

[57] Peter Birks, "The Roman Law Concept of Dominium and the Idea of Absolute Ownership" (1985) Acta Juridica 1, 28.

[58] Koji Takahashi, "Conflict of Laws in Emissions Trading" (2011) 13 Yearbook of Private International Law 145.

[59] James Fawcett & Janeen Carruthers, *Cheshire, North & Fawcett Private International Law* (14th ed., 2008) 794 and 821.

[60] This characterisation seems, however, unsupportable in the context of the Rome II Regulation which contains rules for unjust enrichment (Article 10) because its full title (Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations) indicates that it is concerned with personal remedies rather than proprietary remedies. See e.g. Adeline Chong, "Choice of Law for Unjust Enrichment/Restitution and the Rome II Regulation" (2008) 57 ICLQ 863. For a contrary view, see e.g. Peter Huber (*ed.*) *Rome II Regulation* (2011) Art. 1 para 26

unjust enrichment.[61] Others have argued that the proper characterisation is proprietary on the ground that the issue of whether property is impressed with a trust lies at the heart of such a claim.[62] Whichever characterization is adopted, the governing law is not clear where tokens on a public blockchain are the object of the claim. Thus, we have seen above that the proprietary characterization would not lead to clear choice-of-law rules. The characterization of unjust enrichment would result in the application of the law of the place of enrichment.[63] In the case of transfer to an address on a public blockchain, the place of enrichment is unclear since the blockchain is borderless. This may be contrasted with the case of transfer of deposit to a bank account. The place of enrichment would then be easily identifiable through the geographical location of the branch office with which the account is held.

e. Approach to a uniform law making

We have seen above various circumstances in which proprietary claims may be made to obtain the restitution of blockchain-based tokens. We have found that uncertainty over the availability of such claims is a significant problem. We have further seen a strong case for devising a globally unified solution to that problem. A globally unified solution may be formulated by an instrument in the form of a convention or model law. We will now consider what should be the approach to making a uniform law instrument.

As we have seen, there are divergent legal bases on which proprietary restitutionary claims may be made under the existing legal systems. Thus, some legal systems allow a claim for *rei vindicatio* based on ownership while others require a similar claim to be framed in the tort of conversion. Some legal systems know the principle of a resulting or constructive trust while others do not. It follows that if a uniform law uses the expression of *rei vindicatio*, it risks alienating States in whose legal systems this concept is unknown. The same is true if a uniform law uses any other terms of art such as the tort of conversion, resulting trust and constructive trust. A uniform law should instead choose neutral terms or, in their absence, use terms in a non-technical sense. Thus, if the English word "ownership" is used, care should be taken not to equate it with a notion of any particular legal system such as the French *propriété*,[64] German *Eigentum*,[65] Japanese *shoyûken*[66] and indeed the English law concept of ownership.[67] Again, if

[Ivo Bach].

[61] See e.g. George Panagopoulos, *Restitution in Private International Law* (2000) 70.

[62] See e.g. Adeline Chong, "The Common Law Choice of Law Rules for Resulting and Constructive Trusts" (2005) 54 ICLQ 855.

[63] See Christopher v Zimmerman (2001) 192 DLR (4th) 476 (British Columbia Court of Appeal).

[64] Article 544 of the French Code civil.

[65] Section 903 of the German BGB (Civil Code).

the expression “proprietary restitutionary claim” is used, the uniform law should steer clear of the dogmatic debate in English law over whether its cause of action is unjust enrichment or the vindication of a property right.[68] This stance would also accommodate the legal systems, typically civil law systems, which do not grant proprietary remedies in response to unjust enrichment.[69]

By choosing neutral terms or using terms in a non-technical sense, a uniform law can avoid getting mired in doctrinal debates prevailing in the existing legal systems. There is indeed no need for a uniform law to address the issues involved in the claims of different legal bases as identified in the foregoing analysis, at any event in the context of the specific domestic legal systems in which they arise. Thus, it is not the task of a uniform law to address whether, for example, the Japanese law concept of *shoyûken* should cover bictoin units. What a uniform law instead should do is to prescribe the results for a selection of circumstances which each legal system should produce.[70] It should thus address whether proprietary restitution should be permitted in such circumstances as those described in Cases 1 to 3 above. Even if it should happen that after a careful consideration, the drafters decide not to grant proprietary restitution in any of such circumstances, it would still be better to enunciate the position than leaving it uncertain.

Once a uniform law has been formulated, the enacting States have options: either (1) work out how to reconcile the prescribed results with its existing legal framework or (2) introduce the uniform law as containing a *sui generis* framework. The option (2) would be difficult if the existing law had already produced legislation or a body of case law on the subject matter. But it may be a viable option with respect to a novel asset like blockchain-based tokens.

Finally, it will be necessary to say a few words about execution procedure. When it comes to the execution of a decision allowing a proprietary claim for the restitution of blockchain-based tokens, it will be necessary to have them transferred to the successful claimant by way of obtaining the private key. The process may encounter difficulties where the defendant resists disclosing the key. In some legal systems, a compulsory mechanism such as the threat of

[66] Article 206 of the Minpo (Japanese Civil Code).

[67] It is an elusive concept but is conventionally defined as the residue of legal rights in an asset remaining in a person after specific rights over the asset have been granted to others. See Ewan McKendrick & Roy Goode, *Goode on Commercial Law* (4th ed. 2010) 34.

[68] See e.g. Graham Virgo, *The Principles of the Law of Restitution* (3rd ed., 2015) 7.

[69] George Panagopoulos, *Restitution in Private International Law* (2000) 61.

[70] This approach to a uniform law making is described as a functional approach and favoured by Hideki Kanda, “Methodology of Harmonization and Modernization of Legal Rules on Secured Transactions -- Legal, Functional or Otherwise?” (a paper delivered at the UNCITRAL Fourth International Colloquium on Secured Transactions (2017), available at the UNCITRAL website).

sanctions for contempt of court may be available to compel disclosure. Where the key is stored in a tangible medium such as a hard disc or paper, the seizure of the medium may be possible under some legal systems. It would not be necessary for a uniform law to harmonise this aspect of law since, as with other procedural issues, the method of execution may be left to the *lex fori, i.e.* the law of the place where the procedure is to be taken.

6. Concluding remarks

The legal issues which we have examined above are diverse. Some of them concern the use of distributed ledgers generated by the blockchain technology such as the legal effects of data messages recorded therein. As well as generating distributed ledgers, the blockchain technology makes it possible to trade tokens online on a P2P basis and hold them without the involvement of intermediaries. Those tokens are an object of unprecedented type. Thus, bitcoin units, for example, only exist conceptually as an entry in a blockchain address. They cannot be copied or stored in a tangible medium since there is no such thing as a string of alphanumeric characters for each of the units: what can be stored is rather the private keys to reassign them.[71] Such unique features[72] of blockchain-based tokens are a rich source of novel legal issues.

In the first half of this article, we have examined the existing UNCITRAL works to see what legal issues raised by the blockchain technology may be resolved under them. With principles such as those of technological neutrality and functional equivalence, the existing works are flexible enough to accommodate the blockchain technology. While there are a few unanticipated issues which the technology raises, they may be dealt with by further developing those works.

In the second half of the article, we have examined the circumstances which raise the question whether it is possible to obtain the restitution of blockchain-based tokens by means of proprietary claims. Among the private-law issues arising from the use of the blockchain technology, the uncertainty over the availability of such claims is a problem of particular significance. It also calls for a globally unified solution but is untouched by the existing works of UNCITRAL or any other international organisation. UNCITRAL has a rich experience in the areas of particular relevance such as electronic commerce, insolvency and security interests. It also has a good record of respecting the divergence of existing legal frameworks while at the same time working towards harmonization. All this makes UNCITRAL an ideal and the natural forum for providing a globally unified solution to the problem identified.

[71] Antony Lewis, “A gentle introduction to digital tokens” (https://bitsonblocks.net/2015/09/28/a-gentle-introduction-to-digital-tokens/).

[72] Perkins & Enwezor, *supra* note 54, see certain virtual currencies as a new form of property under English law as they share characteristics of both intangible property and choses in possession.