3. Aspects of private international law related to blockchain transactions

Florence Guillaume

I INTRODUCTION

Blockchain technology (hereafter 'blockchain') is a computer tool that is described as 'the most disruptive tech in decades'.[1] This technology, which is presumably as revolutionary as the Internet, makes it possible to carry out transactions on a digital register, which is often compared to a ledger. The vast majority of transactions based on the blockchain technology (hereafter 'blockchain transactions') take place in an international context. This chapter is about the civil litigation that may result from such transactions. The focus is on private international law rules.

This chapter begins with a short technical explanation of the blockchain technology in Section II. The aim is to outline basic features, which will serve the legal analysis, but are by no means a precise technical description of the blockchain. Section III considers the apprehension of blockchain transactions in private law. The analysis focuses on the current legal framework in order to identify possible unified rules that already exist at the international level. The next section (IV) considers the application of private international law rules to blockchain transactions so as to determine whether these rules are suitable for this type of technology. On the basis of this analysis, proposals of specific private international law rules that could be adopted are formulated in the last section (V).

[1] See *Computerworld*, 'What is Blockchain? The Most Disruptive Tech in Decades' (18 January 2018), accessed 9 February 2018 at https://www.computerworld.com/article/3191077/security/what-is-blockchain-the-most-disruptive-tech-in-decades.html.

II BLOCKCHAIN TECHNOLOGY

The blockchain was originally designed to establish an electronic payment system without any financial intermediary. In 2009, the implementation of the first blockchain was accompanied by the entry into circulation of the first cryptocurrency, bitcoin.[2] The success of this new payment system led to the creation of more than 1,500 other cryptocurrencies, including Ether and Ripple.[3] Cryptocurrencies have a negative aspect, in particular because their inventors often remain unknown. This is the case, for example, with bitcoin, for which the computer program appears to have been created by a person or group of people using a pseudonym.[4] The technology has evolved considerably and is today used for applications extending far beyond a simple payment system.

Before examining the legal treatment of blockchain transactions, we believe it is necessary to provide a brief description of this technology and its main applications so far.

II.A Basic Features of the Blockchain

Blockchain is a shared decentralised database which is distributed among a network of nodes (i.e., a network of computers).[5] The term distributed ledger technology (DLT) is also used to describe this system in which transactions are recorded in multiple places at the same time (i.e., on the various nodes in the network) without a central data store.

In simplified terms, the operation of the blockchain can be described as follows. When a person orders a transaction on the blockchain (e.g., a bitcoin payment), the transaction is initially stored on the nodes of the network in a transaction pool[6] while awaiting validation. The transaction is only completed if an algorithm generated by the software is solved by a node – using its computer power – and its solution is validated by the other nodes. Nodes whose function is to solve the algorithm are known as miners. Algorithms are

---

2 2009 is when the bitcoin source code was first published, and the first block was created.

3 See https://coinmarketcap.com, which listed 1,500 cryptocurrencies in February 2018. The number of cryptocurrencies has tripled in three years; about 500 were listed on the same website in spring of 2015.

4 'Satoshi Nakamoto'.

5 A 'node' is an electronic device that is a part of the network. Each node is running the blockchain software (e.g., the bitcoin software) and participates in the relay of information through the network.

6 This transaction pool waiting to be confirmed is referred to as the 'Memory Pool' on the bitcoin blockchain. See e.g., https://blockchain.info/fr/unconfirmed-transactions, accessed 9 February 2018.

of exponentially increasing difficulty and miners race to solve them because they are remunerated for each one solved. When a miner finds a solution to an algorithm and the solution is confirmed by the majority of other nodes, the transaction is validated and integrated into a new block that is added to the blockchain.[7] This new block is then instantly updated throughout all participating nodes in the network. Since each node maintains a complete copy of the blockchain, there are many identical copies of the blockchain managed in a simultaneous and synchronised manner by all nodes in the network, without any hierarchy among the various copies. The system is collaborative, even community-based, in the sense that a transaction can only be carried out if it is approved by a majority of the members of the network. This is the reason why the blockchain is referred to as a peer-to-peer network.

While bitcoin's 'original blockchain' is a public blockchain, i.e., a network open to anyone wishing to access it, some models of blockchain are private or semi-private,[8] i.e., only open to approved participants. Unlike public blockchains, participation in a private or semi-private blockchain requires an invitation or a permission to join and must be validated by an access control mechanism.[9]

The internal degree of organisation of a blockchain depends on its model. Systems vary from the absence of governance in a public blockchain model, to management by a central administering authority (e.g., an operator of the blockchain) in a private blockchain model, with a whole range of intermediary versions in semi-private blockchain models.

II.B Blockchain as a Payment System

Initially, the blockchain was used solely as an alternative payment system enabling users to avoid using the services of financial intermediaries, in particular banks, credit card companies, Western Union, or PayPal.[10] The objective of this electronic payment system was to enable direct transactions between

---

[7] Only 'full nodes' check the transaction against the blockchain rules and keep a copy of the blockchain. A block can contain one or more transactions. As of today, a block of the bitcoin blockchain contains 1,000 transactions for a maximum size of 1 MB.

[8] Semi-private blockchains are referred to as 'consortium blockchains' or 'hybrid blockchains'.

[9] The access control mechanism can take different forms, such as an authorisation issued by the operator of the blockchain or by other users.

[10] The fundamentals of bitcoin and blockchain technology are discussed in Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System', accessed 9 February 2018 at https://bitcoin.org/bitcoin.pdf.

individuals – for example, cross-border payments – in a secure, quick, and low-cost manner.

Each blockchain is linked to a cryptocurrency which is, so to speak, 'issued' on the blockchain. More precisely, the blockchain produces units of cryptocurrency in order to reward the mining activity. Each algorithm solved enables the miner who found the solution to be rewarded in the cryptocurrency of the network, for example in bitcoins.[11] Cryptocurrencies are neither issued nor controlled by a central regulated authority.[12] They are virtual currencies, which can be defined as 'a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored or traded electronically'.[13] Virtual currencies are not issued physically: they are dematerialised (i.e., they do not have any material form), and are used only for transactions carried out on the Internet, or in the case of cryptocurrencies, on the blockchain.

Cryptocurrencies are not legal tender.[14] However, certain States have created or are considering creating cryptocurrencies indexed to currencies that are legal tender, for example Dubai's emCash, which is indexed to the Emirati dirham.[15] On the other hand, cryptocurrencies can be converted into currencies with legal-tender status (e.g., USD, EUR, CHF). Cryptocurrency rates, in par-

---

[11] The issuance of bitcoins is limited to a maximum of 21 million in order to avoid devaluation. Today, nearly 17 million bitcoins have already been issued. It seems, however, that it will take more than a century to reach the maximum number, given the growing difficulty of mathematical problems that must be solved to validate a block.

[12] See European Central Bank, 'Virtual Currency Schemes – A Further Analysis' (February 2015), 7–11, accessed 9 February 2018 at https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.

[13] Definition in the Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, OJ L 156/43, 19 June 2018 (amendment to Art. 3(18) of the Directive (EU) 2015/849).

[14] State authorities distrust bitcoin, as well as other cryptocurrencies. The hidden nature of these virtual currencies favours their use for illegal purposes (terrorism financing, money laundering, tax evasion, etc.). For example, in September 2017, China ordered the closure of trading platforms for all cryptocurrencies on its territory, before blocking access to platforms in January 2018. Several miners nevertheless remain in Chinese territory.

[15] In Europe, Estonia plans on issuing an estcoin, which would be indexed to the euro.

ticular that of bitcoin,[16] fluctuate very rapidly and unpredictably.[17] The lack of legal-tender status does not prevent the parties to a contract from agreeing that payment must be made in a particular cryptocurrency, for example in bitcoins, which is the most widespread cryptocurrency. It has been observed that bitcoin payments offer users certain advantages:[18] the transaction is validated rapidly – theoretically within around 10 minutes for bitcoin, transaction fees are low,[19] and there are no foreign exchange costs. Companies can also use cryptocurrencies as a financing method. It is increasingly common for start-ups to raise funds by issuing digital tokens in exchange for cryptocurrencies as part of an initial coin offering (ICO).

Cryptocurrencies can only be kept in digital wallets.[20] Users can store their cryptocurrency in a wallet kept on an online platform[21] or on a personal computer, tablet, smartphone, or even in a 'cold wallet', i.e. a wallet which is not connected to the Internet (e.g., in a 'paper wallet' or an offline hardware wallet). It is possible to have one or more wallets, with each wallet being assigned a public key and a private key. This method of asymmetrical cryptography guarantees the security of blockchain transactions. The private key enables users to access their wallet to make a transaction, whereas the public key is used by the network to identify the user.[22] Cryptocurrencies are lost when users are no longer able to access their electronic wallet due to the loss or theft of their private key.

---

[16] For example, in 2017 the price of bitcoin rose from USD 1,000 in January to almost USD 20,000 in mid December, then dropped to USD 6,000 in early February 2018. Since December 2017, and despite the volatility of its price, bitcoin has been traded on the Chicago Mercantile Exchange where it is possible to speculate on the evolution of its price with bitcoin futures.

[17] In 2017, the launch of the tether aimed to remedy the volatility problem of cryptocurrency prices. The idea was to link the price of this cryptocurrency to that of the US dollar: the operator has committed to deposit in a bank account USD 1 for each tether issued. But this system has raised doubts after the issuance of over a billion tethers.

[18] See European Central Bank (supra n 12), 18–20.

[19] Transaction fees can be set freely by users and can significantly fluctuate depending on supply and demand. Transactions for which users offer higher fees are dealt with as a priority by miners. When the blockchain is saturated, transactions offering low transaction fees may be ignored by miners. Bitcoin blockchain saw an increase in transaction fees in 2017, which rose from an average of USD 1 at the beginning of the year to USD 55 at the end of the year.

[20] Electronic wallet software allows the user to create wallets and make transactions on the network.

[21] For example, Coinbase: https://www.coinbase.com.

[22] The keys are encoded and can be represented as a QR code. The private key is kept by the user (it is equivalent to the signature or code of a credit card holder), while the public key is transmitted to third parties to carry out transactions (it is equivalent to an account number or a credit card number).

The blockchain is a public register: each user can see that someone is carrying out a transaction. However, the anonymity of transactions is guaranteed. The only public element is a user's public key, which appears in the blockchain next to each transaction. The identity of the person behind a particular public key is not known to the other users, who are in general unable to make the connection between the public key and the private key that contains the personal information. But the anonymity is not absolute. The other party to a transaction may know the identity of the holder of a public key, for example when buying clothes on a website with bitcoins. In this case, the seller not only knows the buyer's personal information, but may also find out his or her digital wallet's balance by tracing all of the transactions made by this person in bitcoins, which are freely accessible in the blockchain ledger.[23] Indeed, the blockchain contains a record of each and every transaction ever made in the system: anything recorded in the blockchain is permanent and can never be erased.[24]

II.C Other Applications of the Blockchain

Blockchain applications are highly varied and constantly developing.[25] Some examples will demonstrate the potential of this technology, which is already bringing changes in the way several sectors of the economy operate.

Smart contracts have been one of the most interesting developments of the blockchain.[26] They are computer codes embedded with if/then statements that are executed by the software when the conditions previously defined in the code are met. For example, a smart contract can be used to 'back up' a sales agreement (i.e., the base contract), which provides for a payment to be made on a certain date; the payment (i.e., the execution of the smart contract) will be automatically triggered on that particular date without any action being required from the parties. By necessity, the smart contract is executed in accordance with the code, which cannot be modified once it has been recorded in the blockchain. The performance of the base agreement between the parties

---

[23] Laurent Leloup, *Blockchain – La révolution de la confiance* (Eyrolles, 2017), 50–2.

[24] The blockchain transaction is, so to speak, set in a 'block' of stone.

[25] See *Fortune*, 'Here's Why Blockchains Will Change the World' (8 May 2016), accessed 9 February 2018 at http://fortune.com/2016/05/08/why-blockchains-will-change-the-world ('The new platform enables a reconciliation of digital records regarding just about everything in real time'). See also Aaron Wright and Primavera De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia', SSRN, March 2015, 8–17, accessed 9 February 2018 at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.

[26] For example, https://www.ethereum.org, which is a blockchain application platform offering many types of blockchain applications using smart contracts.

is thus guaranteed by the system, which makes it – at least in theory – 100 per cent reliable. In addition, smart contracts provide a digital, forge-proof, and dated record of the agreement between the parties as a result of being recorded in the blockchain. Smart contracts thus enable the terms of the base contract to be recorded in the blockchain and, thereby, stored securely.

The recording ability of the blockchain is useful for storing any type of information in a secure manner. This technology can be used in identity management systems to record personal data. For example, it enables the storage of patient medical records while automatically paying health professionals after a medical consultation. The blockchain can also be used for the purposes of certification or authentication, since it fully meets the requirements of public registers, such as the register of births, marriages and deaths, the land register, or the company register.[27]

There are many other possibilities for using the blockchain, in particular any product or service that may benefit from the security and transparency offered by this technology. It may be used to ensure the traceability of a product or material throughout its production and distribution chain, for example food products.[28] The blockchain can also be used as evidence. It essentially supplies proof that a transaction has occurred. This makes it appealing to the raw materials industry, which sees in it a simple and effective way to replace the cumbersome approval of paper documents with the fast, secure, and economical process of electronic validation.[29] In the shipping sector, for example, the payment can be executed by a smart contract as soon as a shipment is delivered. The use of the blockchain enables payment to be triggered automatically as soon as receipt of the goods is confirmed; this confirmation can come from a person or even without human intervention, for example when the goods are

---

[27] Sweden, for example, has already switched to a blockchain-based register system. Other countries are implementing this technology for their land register, for example India, Brazil, and Honduras. In Switzerland, the Canton of Geneva is testing a blockchain company register.

[28] For example, the supermarket chain Walmart uses blockchain technology to improve food tracking and safety in China. See *forbes.com*, 'IBM & Walmart Launching Blockchain Food Safety Alliance in China with Fortune 500's JD.com' (14 December 2017), accessed 9 February 2018 at https://www.forbes.com/sites/rogeraitken/2017/12/14/ibm-walmart-launching-blockchain-food-safety-alliance-in-china-with-fortune-500s-jd-com/#3c10a367d9c5b.

[29] See *Le Temps*, 'Des négociants à Genève s'allient pour imposer la blockchain' (10 November 2017), accessed 9 February 2018 at https://www.letemps.ch/economie/2017/11/10/negociants-geneve-sallient-imposer-blockchain; Computerworld, 'Maersk, IBM Create World's First Blockchain-based, Electronic Shipping Platform' (16 January 2018), accessed 9 February 2018 at https://www.computerworld.com/article/3247758/emerging-technology/maersk-ibm-create-worlds-first-blockchain-based-electronic-shipping-platform.html.

equipped with a GPS so that their location can be verified and this information transmitted directly to the system.

In the public sector, several States are using the opportunities offered by the blockchain to make the shift to digital administration. For example, Estonia has been using a blockchain-based ledger for government services for several years now. Dubai is planning various applications of blockchain technology across government services, which since 2017 can be paid for in emCash. Great Britain is currently examining the possibility of using the technology in such sectors as national security and public safety, healthcare, cybersecurity, and customs and immigration.[30] In Switzerland, the city of Zug recently launched a pilot project using blockchain-based digital ID.[31]

For the analysis that follows, it should be borne in mind that there are various applications of the blockchain with very different characteristics. Some statements may therefore be valid for certain types of blockchains but not for others.

III BLOCKCHAIN TRANSACTIONS AND PRIVATE LAW

On the international stage, it may be observed that certain States are frantically attempting to establish a position within the digital economy and racing to attract companies using the blockchain.[32] However, at the time of writing, there are to our knowledge no private law rules adopted by any State[33] or group of States that apply specifically to blockchain transactions. This (apparent) legal vacuum has not prevented the enthusiastic development of commercial oper-

---

[30] See House of Lords, 'Distributed Ledger Technologies for Public Good: Leadership, Collaboration and Innovation', accessed 9 February 2018 at http://chrisholmes.co.uk/wp-content/uploads/2017/11/Distributed-Ledger-Technologies-for-Public-Good_leadership-collaboration-and-innovation.pdf.

[31] See http://www.stadtzug.ch/de/bevoelkerung/dienste/digitaleid (accessed 9 February 2018).

[32] 'Blockchain friendly' labels can be seen flourishing everywhere. For example, the Swiss Canton of Zug has proclaimed itself the Crypto Valley. See *Blick*, 'Reisewelle ins Krypto-Valley Zug' (31 December 2017), accessed 9 February 2018 at https://www.blick.ch/news/schweiz/zentralschweiz/chinesen-und-amerikaner-wollen-schweizer-blockchain-boom-hautnah-erleben-reisewelle-ins-krypto-valley-zug-id7787875.html.

[33] Several projects are currently under study. For example, Monaco is considering a Blockchain Act ('*Proposition de loi relative à la blockchain*'), accessed 9 February 2018 at www.conseil-national.mc/index.php/textes-et-lois/propositions-de-loi/les-propositions-de-loi-en-cours/item/600-237-proposition-de-loi-relative-a-la-blockchain.

ations using this technology. The lack of regulation exposes users to a wide range of economic and legal risks.

For the purposes of this study, our position is that the growing number of blockchain users requires a legal framework that is as clear as possible. First of all, we must therefore establish whether the current legal framework is sufficient to accommodate the questions of private law raised by the use of this technology.

III.A Legal Scope of Blockchain Transactions

We will focus our attention on the private law questions that may arise during blockchain transactions. The first task is to determine whether this type of transaction has any legal scope. Does the use of this technology have any effect on the legal force of the rights and obligations that are assumed to arise from a transaction? This question must be settled by each State through the exercise of its sovereignty.

For example, when a State uses blockchain technology for its land register, the law of this State must define the legal scope of the transactions recorded in the blockchain. The law must determine whether the legal scope of the computer code is limited to proof of the property right, or whether it is wider, by establishing the code as one of the conditions for acquiring the property right of immovable property, or wider still, by considering the code as the property deed.

But the topic of choice when it comes to measuring the legal scope of blockchain transactions is the smart contract. This application of the blockchain has been the subject of much investigation, in particular due to the use of the word 'contract'.[34]

When the blockchain is used 'in support' of an agreement reached between the parties, for example when the performance of a sales agreement is provided for by a smart contract, the main difficulty lies in the relationship between the agreement reached between the parties (i.e., the base contract) and the code

---

[34] The concept of 'smart contract' is attributed to Nick Szabo, '"Smart Contracts": Formalizing and Securing Relationships on Public Networks', 2(9) *First Monday*, 1 September 1997, accessed 9 February 2018 at http://firstmonday.org/article/view/548/469. This terminology is disputable. See Eliza Mik, 'Smart Contracts: Terminology, Technical Limitations and Real World Complexity', (2017) 9(2) *Law, Innovation and Technology*, 269–300. ('The seminal paper itself abounds in legal terminology, creating an impression that its propositions are grounded on solid legal principles. Most concepts described therein are, however, misrepresented. What follows is a morass of technological and legal jargon, which is endlessly recycled in subsequent technical writings', at 273).

recorded in the blockchain (i.e., the smart contract). The distinctive feature here is that the computer code is a transcription into the virtual world of the contract entered into in the real – physical – world. In a sense, the computer environment is superimposed on the legal environment. Should smart contracts be recognised as having a legal scope independent of that of the base contract, or on the contrary, should they be considered merely as a means of executing the base contract?

In our opinion, it is impossible to provide a general answer to this question: we must distinguish between the different situations where smart contracts are used. The smart contract is, in fact, not always a transcription of the base contract. It may go beyond the terms of the base contract and incorporate contractual terms not provided for in the base contract. Further, there is nothing preventing the parties from simply formalising their agreement via a smart contract, without connecting the 'virtual contract' to an underlying 'real contract'. A smart contract can even be created 'spontaneously' by the blockchain, for example in order to follow up on the execution of an initial smart contract. In such situations, the smart contract can no longer be considered merely a transcription of the base contract into the computer environment.

The smart contract creates – or not – its own legal effects, which are imposed upon the parties depending on how smart contracts are perceived in the legal order in question. It has been observed that the code – i.e., the smart contract – is self-executing and from this perspective has legal effect ('code is law').[35] In any case, the contract must be inevitably executed in accordance with the code, which therefore has binding effect.[36] We believe it is too simplistic to consider that smart contracts are developed solely in a computer environment that is entirely disconnected from the real world and have thus no legal scope. Nor is it possible to make the general assertion that all smart contracts have legal effect.[37] But the use of smart contracts raises an additional question: with which legal order is the smart contract connected? In other words, which State has jurisdiction to determine whether the blockchain transaction has a legal scope?

---

[35] See Lawrence Lessig, *Code and other laws of cyberspace* (Basic Books, 1999), 3–8 (and the same, *Code version 2.0* (2nd edn., Basic Books, 2006), 1–8.

[36] See Florian Glatz, 'What are Smart Contracts? In Search of a Consensus', accessed 9 February 2018 at https://medium.com/@heckerhut/whats-a-smart-contract-in-search-of-a-consensus-c268c830a8ad ('It is however undeniable, that smart contracts have to be classified as legally relevant behaviour').

[37] Same opinion: Mik (supra n 34), 285–6.

III.B International Scope of Blockchain Transactions

Use of the blockchain forms part of the broader use of the Internet. As a tool designed to be ubiquitous and universal, the Internet is not only dematerialised; it is also intrinsically transnational. By definition, its use knows no borders. The same applies to the blockchain.

The international nature of the blockchain results, in particular, from the role of the nodes. It is statistically unlikely that all the nodes in the network, which maintain an identical copy of the blockchain, will be located in a single State. Even if we focus on a single transaction, whose validation requires a miner to find the solution to the algorithm and a majority of nodes to confirm this solution, it is statistically unlikely that all the nodes involved in this transaction will be located in the same State. Additionally, the involvement of a node in a transaction is entirely random and impossible to predict in advance. It is also extremely difficult to identify the nodes that actually participated in a specific transaction.

That is why we believe that the use of the blockchain is enough to give the transaction an international scope. The only exception would be the situation in which all nodes, all the users, as well as the operator of the blockchain are located in the same State. We must therefore begin from the assumption that all blockchain transactions must be considered international by nature. Since each blockchain transaction raises the question of which legal order has competence to grant it legal scope, each transaction contains a potential conflict between the laws of different States.

From an international perspective, it should first be established whether there are any uniform rules of law at the international level that may apply – at least by analogy – to blockchain transactions. It should be noted in this regard that States have not yet adopted uniform private law rules for all legal relationships formalised via the Internet. International institutions have begun examining the issue of the normative environment of the Internet, in particular in the realm of electronic commerce, by proposing model laws[38] and recommendations.

This legal work is based, in particular, on the guiding principle of technological neutrality. This principle mandates the adoption of legal provisions that are neutral with respect to the technology used. This ensures that the law is able to accommodate any future technological development. The rules of law adopted

---

[38] For example, the United Nations Commission on International Trade Law (UNCITRAL) focused on the harmonisation of national legislation on e-commerce, particularly through the development of the UNCITRAL Model Law on Electronic Commerce: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html (accessed 9 February 2018).

for transactions carried out on the Internet can therefore (in theory) be applied to legal questions arising in relation to the use of the blockchain, even if this technology had not yet been invented when these rules were adopted. For example, Article 12 of the United Nations Convention on the Use of Electronic Communications in International Contracts[39] may be useful for interpreting the formation of smart contracts. According to this rule, '[a] contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract'. One could infer from this provision that smart contracts could be considered valid so long as such transactions can be qualified as contracts in the legal sense of the term. However, the principle of technological neutrality is highly theoretical, as demonstrated by cloud computing contracts, which are currently the subject of a study seeking to develop specific rules for the use of this technology.[40]

Even if blockchain transactions – just like those made on the Internet more generally – might benefit from the uniformisation of the rules of private law at the international level, it must be acknowledged that these rules are still very disparate and insufficient to govern every question of private law raised by the use of these technologies. It is therefore the responsibility of States to determine the legal scope of blockchain transactions by legislating within the limits of domestic law. Insofar as domestic laws differ from one State to another, this creates a degree of legal uncertainty.

IV BLOCKCHAIN TRANSACTIONS FROM A PRIVATE INTERNATIONAL LAW PERSPECTIVE

The lack of uniform private law rules adopted at the international level makes it necessary to apply the rules of private international law in order to determine the applicable law for blockchain transactions. The rules of private international law are intended to remedy legal uncertainty by connecting a particular legal relationship with the legal order of a State. These rules are extremely important, as they enable the participants in a blockchain to deter-

---

[39] See http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html accessed 9 February 2018.

[40] See UNCITRAL, 'Contractual aspects of cloud computing (2018)', accessed 9 February 2018 at https://documents-dds-ny.un.org/doc/UNDOC/LTD/V18/003/89/PDF/V1800389.pdf?OpenElement.

mine in advance and with certainty which State's law governs their rights and obligations.

One may question whether private international law is able to apprehend legal relationships formalised via the Internet. The traditional approach used for connecting a legal situation to a legal order aims to determine the seat of the legal situation.[41] The rules of private international law are designed to make it possible to determine the State with which the issue at hand has the closest connection. The objective is therefore to establish the geographical location of legal relationships. The method does not appear appropriate, insofar as the Internet – like the blockchain – is an inherently intangible and transnational phenomenon. It is therefore extremely difficult to establish the location of a transaction made on the Internet, let alone the blockchain. This is why States have not yet taken steps to unify the rules of private international law applicable to digital activities via a multilateral international convention.

In the absence of uniform private international law rules adopted at the international level, domestic conflict-of-law rules are applied to determine the law applicable to blockchain transactions.

IV.A Application of Swiss Private International Law Rules to Blockchain Transactions

In this section, we will examine blockchain transactions using the tools available in Swiss private international law. Like Swiss substantive law, Swiss private international law does not yet contain dedicated rules for blockchain transactions. However, the absence of specific rules does not necessarily mean that blockchain transactions cannot be apprehended by private international law. Other rules may in fact apply to these transactions, by analogy if necessary. Establishing the legal qualification of blockchain transactions will make it possible to assign them to one of the categories of Swiss private international law, in order to determine the applicable conflict-of-law rules.

We will examine several situations in order to compare the existing conflict-of-law rules with the legal issues arising from blockchain transactions. This study will enable us to determine whether existing conflict-of-law rules offer satisfactory solutions for blockchain transactions. At this stage, our analysis will focus on the rules enabling the determination of the applicable law.

---

[41] See Friedrich Karl von Savigny, *System des heutigen römischen Rechts*, Vol. 8 (Berlin 1849). See also Andreas Bucher, *La dimension sociale du droit international privé – Cours général* (ADI-Poche, 2011), 48–65.

IV.A.1 Determining the law applicable to cryptocurrency theft

The first example concerns the theft of cryptocurrencies, which is common and affects both users and miners.[42] The malicious act consists of stealing the cryptographic keys, for example by hacking the exchange platform.[43] The hacking can cause the company hosting the platform to abruptly stop its activities, entailing a significant risk for users of losing their digital wallet.[44] This leads to the issue of whether the user is able to recover his or her cryptocurrencies or an amount corresponding to their value in the insolvency proceeding of the company hosting the platform.

One must determine the appropriate qualification of cryptocurrencies before answering this question. Much debate surrounds the nature of the right enjoyed by a cryptocurrency's holder: is it a right *in rem* or a right *in personam*? Does the holder of the digital wallet have ownership of things, or does the holder have a claim against the company hosting the platform? The categories defined in the Swiss Private International Law Act (SPILA) are largely inspired by the categories of private law established mainly by the Swiss Civil Code (SCC) and the Swiss Code of Obligations (SCO). Under Swiss law, only things, traditionally considered to mean material objects, can be the subject of a right *in rem*.[45] Exceptionally, in cases defined by the law, a right *in rem* may also apply to a right, meaning that the rules on rights *in rem* can be applied by analogy. Under current Swiss law, cryptocurrencies do not fall within the definition of things that can be the subject of a right *in rem*.[46] In our view,

---

[42] For example, the miner NiceHash had more than 4,000 bitcoins stolen in December 2017, worth about USD 63 million.

[43] For example, the Bitfinex cases in 2015 and 2016, the Gatecoin case in 2016, the Youbit case in 2017. See *Les Echos*, 'Les cybercasses se succèdent dans le monde du bitcoin' (20 January 2018), accessed 9 February 2018 at https://www.lesechos.fr/finance-marches/marches-financiers/0301109412054-les-cybercasses-se-succedent-dans-le-monde-du-bitcoin-2146641.php.

[44] For example, the Mt Gox case in 2014 and the Coincheck case in 2018.

[45] Art. 641 SCC states that: '(1) The owner of a thing is free to dispose of it as he or she sees fit within the limits of the law. (2) He or she has the right to reclaim it from anyone withholding it from him or her and to protect it against any unwarranted interference.'

[46] This is a controversial question in Swiss law, but the majority of the authors reject the qualification of cryptocurrencies as a thing. See Benedikt Maurenbrecher and Urs Meier, 'Insolvenzrechtlicher Schutz der Nutzer virtueller Währungen', *Jusletter*, 4 December 2017, 6–7 (with further references); Stephan D. Meyer and Benedikt Schuppli, '"Smart Contracts" und deren Einordnung in das schweizerische Vertragsrecht', *Recht* (2017), 204–24, at 219–21; Gabriel Olivier and Benjamin Jaccard, 'Smart Contracts and the Role of Law', *Jusletter* IT, 23 November 2017, 12; Martin Hess and Stephanie Lienhard, 'Übertragung von Vermögenswerten auf der Blockchain', *Jusletter*, 4 December 2017, 11–12.

they are book-entry securities and can only be considered as claims. However, this qualification raises practical issues which are worth resolving, either by extending the notion of a 'thing' to digital property or via specific provisions on cryptocurrencies, in particular in the event of bankruptcy of the company hosting the platform.

For the sake of demonstration, let us assume that the holder of cryptocurrencies has a right in rem, and can therefore assert his right through an action relating to personal property rights.[47] This action enables the holder to recover the cryptocurrencies (e.g., the bitcoins) that were stolen from him or her, if the thief can be identified. The acquisition and loss of personal property rights are governed by the law of the place where the personal property is located at the time of the facts on which the acquisition or loss is based.[48] This rule makes it possible to establish the geographical location of the legal relationship: the location of the property is that with which the relationship has the closest connection. The application of *lex rei sitae* to property law is a classic rule of private international law that is found in the law of most countries. Admittedly, application of this rule requires locating the digital wallet emptied by the thief, which in our view means locating the private key of the victim. This location cannot really be transposed from the virtual world into the real world.[49] In our opinion, the location of the wallet is too random to constitute a useful connecting factor to establish the location of the stolen cryptocurrencies. The wallet may indeed be kept in various ways, online and offline (e.g., on an online platform, a personal computer, an offline hardware wallet, a 'paper wallet'). The way the wallet is kept cannot be relevant for determining the applicable law. Establishing the location of the cryptocurrency by tying it to the location of the holder's private key does not therefore provide a satisfactory solution in private international law. The connecting factor of *lex rei sitae* does not

---

[47] Swiss law provides for an action relating to personal property rights in Art. 641(2) SCC (see supra n 45). For an analysis of Swiss law, see Barbara Graham-Siegenthaler and Andreas Furrer, 'The Position of Blockchain Technology and Bitcoin in Swiss Law', *Jusletter*, 8 May 2017, 11–18; for a comparative approach, see Koji Takahashi, 'Implications of the Blockchain Technology for the UNCITRAL Works', 11–17, accessed 9 February 2018 at https://onedrive.live.com/?authkey=%21AMLDDJc03VocQms&cid=431D6C57123F90CF&id=431D6C57123F90CF%212163&parId=root&o=OneUp.

[48] Art. 100(1) SPILA.

[49] Raskin's proposition that bitcoins are located in the territory of a state if that state 'can exercise power over a private key by transferring the bitcoins into the court's wallet' does not seem relevant to us outside the US judicial system. See Max Raskin, 'Realm of the Coin: Bitcoin and Civil Procedure' (2015) 20(4) *Fordham Journal of Corporate and Financial Law* 969–1011, at 1003.

make it possible to establish the law applicable to the acquisition and loss of cryptocurrencies.

Let us now ascertain whether qualifying the right of the holder of cryptocurrencies as a right *in personam* is any more convincing under private international law. In most cases, the cryptocurrencies are kept on an online platform and the injured holder tries to obtain reimbursement and/or compensation from the company hosting the platform in the event of theft. Let us leave this legal relationship aside – which is essentially governed by the user agreement[50] – and examine the legal means available to the holder of the cryptocurrency for asserting his or her right via an action in tort against the thief.[51] This action enables the holder to recover an amount of money corresponding to the amount of cryptocurrency stolen, if the thief can be identified. Claims in tort are governed by the law of the State in which the tort was committed or in which the result occurred if the tortfeasor should have foreseen that the result would occur there.[52] This rule again makes it possible to establish the geographical location of the legal relationship: the place of the tort, or the place where the result of the tort occurred, is that with which the relationship has the closest connection. The application of *lex loci delicti* is a classic rule of private international law that is found in the law of most countries. Application of this rule requires establishing where the theft occurred, which in our view means the location where the hacking took place. The hacker may have acted from any location, or even from several locations if several hackers coordinated their efforts. Locating the place in which the tort was committed may therefore prove extremely difficult and may result in the application of a variety of different laws. Furthermore, this rule could have the additional disadvantage that the hacker has chosen to act from a country in which the theft of cryptocurrencies is not considered to be illegal. Establishing the place of the result of the tort means locating the digital wallet emptied by the hacker, which in our view brings us back to locating the private key of the victim. As we have seen, establishing this place does not provide a satisfactory solution in private international law since this place is too random. It is therefore impossible to establish a specific connection with a precise place in the case of a tort committed on the blockchain. This example shows that the criteria used to establish the place where the tort occurred are not suited to this technology.

---

[50] See e.g., Coinbase user agreement, https://www.coinbase.com/legal/user_agreement accessed 9 February 2018.

[51] Under Swiss law, the action in tort is provided for in Art. 41 SCO: '(1) Any person who unlawfully causes loss or damage to another, whether wilfully or negligently, is obliged to provide compensation. (2) A person who wilfully causes loss or damage to another in an immoral manner is likewise obliged to provide compensation.'

[52] Art. 133(2) SPILA.

The theft of cryptocurrencies is distinctive in that there is not necessarily an online interaction between the hacker and the victim. For example, the electronic communication devices of the holder of the cryptocurrencies are not directly affected by the hacking if the theft occurs on an online platform. Likewise, when the cryptocurrencies are stored in a 'paper wallet', or even an offline hardware wallet, there is not necessarily an online interaction between the hacker and the victim. However, the theft of cryptocurrencies as such always requires the use of the Internet. This feature is a more decisive factor for determining the State with which the theft of cryptocurrencies has the closest connection than the location where the hacking took place or the location of the private key of the victim.

One could wonder if the physical location of the person whose cryptocurrencies were stolen is of any importance for the search of the law applicable to cryptocurrency theft. Swiss private international law refers to this factor in order to determine the law applicable to claims in tort when the tortfeasor and the injured party have their habitual residence in the same State. This is rarely the case in practice when cryptocurrencies are stolen.[53] The law of the State in which the injured party has its habitual residence or its domicile could also be considered as a connecting factor if the rules related to infringement of personal rights could apply by analogy or if the presence of a legislative gap could be recognised.[54] In our opinion, the place where the holder of cryptocurrencies has his or her habitual residence or domicile does not provide a satisfactory solution in private international law since he or she may connect to the Internet from anywhere and may therefore theoretically access his or her digital wallet from any location.

It can be concluded that Swiss conflict-of-law rules cannot be used to determine the applicable law in a satisfactory manner in the event of cryptocurrency

---

[53] Art. 133(1) SPILA states that: 'When the tortfeasor and the injured party have their habitual residence in the same State, claims in tort are governed by the law of such State.'

[54] Art. 33 SPILA states that: '(1) Whenever this Act does not contain specific provisions, … matters pertaining to the status of individuals [are governed by] the law of the domicile. (2) However, infringement of personal rights are governed by the provisions of this Act relating to torts …' The law of the domicile of the holder of cryptocurrencies could therefore apply only if a legislative gap could be recognised. Under Art. 139(1) (a), 'Claims based on the infringement of personal rights by the media, including press, radio, television or any other public information medium, are governed at the option of the injured party: (a) by the law of the State in which the injured party has his or her habitual residence, provided the tortfeasor should have expected that the result would have occurred in that State; …'. The law of the habitual residence of the holder could therefore apply only if the theft of cryptocurrencies could be qualified as an infringement of personal rights by the media, which is dubious.

theft, regardless of the qualification used. The conflict-of-law rules on rights *in rem*, just like those relating to tort, ueed to be adjusted or at least reinterpreted in light of the distinctive features of the blockchain.

IV.A.2 Determining the law applicable to smart contracts

The second example concerns the use of smart contracts, which will enable us to examine several scenarios.

Firstly, let us consider the example of a money loan contract entered into by two persons, where the lender is domiciled in Switzerland and the borrower in Singapore. The parties agree that the loan must be repaid in ethers. If the borrower does not repay by the agreed date and the lender wishes to force him or her to pay, the first question is whether the fact of agreeing to a payment in ethers is legally binding. The answer depends on the law applicable to the agreement. Contracts are generally governed by the law chosen by the parties.[55] Failing a valid choice of law, contracts are governed by the law of the State with which they have the closest connection.[56] For a money loan contract, the law assumes that the State in which the lender has his or her habitual residence is that with which the contract has the closest connection.[57] Under Swiss law, cryptocurrencies are not legal tender.[58] A creditor is therefore under no obligation to accept payment in cryptocurrency. On the other hand, the parties can agree on the means of payment without it necessarily being a currency with legal-tender status. Payment in ethers can therefore be validly agreed upon by the parties.[59] As is the case here, the agreement of the parties on this point is legally binding.

If the parties have used a smart contract to 'back up' this loan contract, for example by providing for the automatic repayment of the loan on the agreed deadline, the smart contract has the effect of transposing the base contract into the virtual world. The performance of the contract is therefore simplified and does not (in theory) involve any risk, since the payment will be automatically triggered on the agreed deadline. But the risk of error in smart contracts is not zero. Assuming that the computer program itself is infallible, the risk of error is concentrated in the phase in which the base contract is 'transformed'

---

55 Art. 116(1) SPILA.

56 Art. 117(1) SPILA.

57 Art. 117(2) and (3)(b) SPILA.

58 See Art. 2 of the Federal Act on Currency and Payment Instruments. See also Conseil fédéral, Rapport sur les monnaies virtuelles en réponse aux postulats Schwaab (13.3687) et Weibel (13.4070) (25 June 2014), 7, accessed 9 February 2018 at https://www.news.admin.ch/NSBSubscriber/message/attachments/35353.pdf.

59 See Mirjam Eggen, 'Verträge über digitale Währungen', *Jusletter*, 4 December 2017.

into a smart contract. The computer code is not spontaneously entered into the blockchain: the involvement of a physical person is (still) required to retranscribe the contract onto the blockchain. The code may therefore contain an error. This risk is all the greater since it is impossible for a legal expert without detailed knowledge of computer programming to verify that the code corresponds in fact to the agreement between the parties.[60]

In addition, there is a risk that the smart contract will be executed in a manner that does not correspond to the expectations or wishes of the parties – or at least of one of the parties – even when the code does correspond to the base contract. In this case, the parties are faced with an incorrect execution of the base contract as a result of the programme logic. This risk exists insofar as it is difficult to include all the elements of the base contract in the computer code, in particular concepts requiring a degree of subjectivity or interpretation.[61] The principle difficulty relating to codification[62] of the base contract is determining the person responsible for the error. This question is settled either by the parties in the provisions of the base contract, or by the law applicable to the contract. It will then be up to the responsible party to take action against the programmer, if he or she can be identified. The responsibility of the programmer will then be determined either contractually or by reference to the applicable law.

For the same loan contract, let us examine a scenario where a payment in ethers is erroneously made to the digital wallet of a third party due to an error in the code of the smart contract. If this person can be identified, he or she may be required to return the mistakenly transferred ethers under the rules on unjust enrichment.[63] The law applicable to this legal relationship is the law of the State in which the enrichment occurred.[64] In the case of enrichment resulting

---

[60] There is no reliable computer means of allowing the transcription of natural language into code yet. We can assume, however, that this difficulty will be resolved in the near future.

[61] See Scott Farrell, Heidi Machin and Roslyn Hinchliffe, 'Lost and found in Smart Contract Translation – Considerations in Transitioning to Automation in Legal Architecture', accessed 9 February 2018 at http://www.uncitral.org/pdf/english/congress/Papers_for_Programme/14-FARRELL_and_MACHIN_and_HINCHLIFFE-Smart_Contracts.pdf; Rolf H. Weber, 'Leistungsstörungen und Rechtsdurchsetzung bei Smart Contracts', *Jusletter*, 4 December 2017, 11–13; Meyer and Schuppli (supra n 46), 217–18; Mik (supra n 34), 287–98.

[62] That is, the 'code-ification' of the contract.

[63] Under Swiss law, the action for unjust enrichment is provided for in Art. 62 SCO: '(1) A person who has enriched himself without just cause at the expense of another is obliged to make restitution. (2) In particular, restitution is owed for money benefits obtained for no valid reason whatsoever, for a reason that did not transpire or for a reason that subsequently ceased to exist.'

[64] Art. 128(2), 1st sentence, SPILA.

from an erroneous money transfer, this generally means the State in which the enriched third party is domiciled. In our view, this rule can be applied by analogy to cryptocurrencies. The restitution of ethers can only be ordered if permitted by the law of this State. If this is not the case, for example if the law of this State does not recognise the validity of cryptocurrency transactions, the question then arises whether a Swiss judge can apply Swiss law to order the restitution. In any case, this does not appear to be a situation justifying the application of public policy[65] or the exception clause.[66] The parties may agree to apply Swiss law,[67] but the agreement of the enriched party may be difficult to obtain in practice.

If the smart contract is not simply a codification of the loan contract, but instead goes beyond the terms of the base contract, for example by setting out additional contractual terms, the reasoning will be the same as when the smart contract is simply a transcription of the base contract. However, the smart contract can only produce its own legal effects if it is a legally binding agreement under the law governing the contract. For example, a smart contract governed by Swiss law can only have legal effects if the Swiss legal order recognises its legal existence.[68] A choice of law in favour of the law of a State that recognises the legal existence of smart contracts will enable the parties to avoid the risk of the smart contract having no legal effect. In our opinion, the effects of a choice of law contained in the base contract should in principle extend to the smart contract. If the contract is governed by foreign law, the recognition in Switzerland of the legal effects of the smart contract (assuming these are valid under the law governing it) will only be compromised if this would lead to a result that is incompatible with Swiss public policy.[69]

The situation becomes more complicated when a smart contract is entered into on the blockchain independently of any base contract. If the smart contract does not 'back up' a base contract, the legal framework is established solely in the smart contract, in other words in the computer code. In this case, it is no longer possible to refer to an underlying base contract existing outside the

---

[65] According to Art. 17 SPILA: 'The application of provisions of foreign law is excluded if such application leads to a result that is incompatible with Swiss public policy.'

[66] According to Art. 15 SPILA: '(1) As an exception, any law referred to by this Act is not applicable if, considering all the circumstances, it is apparent that the case has only a very loose connection with such law and that the case has a much closer connection with another law. (2) This provision does not apply where a choice of law has been made.'

[67] Art. 128(2), 2nd sentence, SPILA.

[68] See Olivier and Jaccard (supra n 46), 216–18; Andreas Glarner and Stephan D. Meyer, 'Smart Contracts in Escrow-Verhältnissen', *Jusletter*, 4 December 2017, 7–8.

[69] Art. 17 SPILA (see supra n 65).

computer environment. In the event of breach of contract, each of the parties to the contract can initiate legal proceedings if he or she knows the identity of the other party. This question risks being unsolvable in practice, as it is not always possible to identify the other users of the blockchain.

Additionally, it must be taken into account that it could be possible for a smart contract to be created 'spontaneously' by the blockchain. In this case, the contract is concluded via electronic agents, i.e. computer codes. The role of electronic agents in the negotiation and formation of contracts is not clear from a legal point of view, as different approaches on the legal effect of smart contracts have emerged.[70] It may at least be considered that the computer code does not act as a simple messenger expressing a party's will, but rather acts as an agent contracting in the name of the principal. It will be all the more difficult to identify the contracting parties in this type of smart contract. In the absence of specific private international law rules on legal relationships formalised via the blockchain, the court will determine the applicable law after having qualified the legal relationship between the parties.

Our examination of these scenarios reveals that the application of Swiss conflict-of-law rules where a smart contract is in use makes it possible to determine the applicable law in a satisfactory manner, at least when the parties to the base contract have chosen the applicable law. However, the situation becomes more complicated when there is no underlying base contract, as in this case it is necessary to determine which law is applicable to the smart contract and whether this law attributes legal effects to relationships formalised solely via the blockchain.

IV.B In Search of the Location of the Blockchain Transactions

Taking the rules of Swiss private international law as our yardstick, we can conclude that the rules adopted before the appearance of blockchain are difficult to apply to this technology. The examples of cryptocurrency theft and the use of smart contracts have shown that the existing rules of private

---

[70] See Bettina Mielke and Christian Wolff, '"Klar ist der Aether und doch von unergründlicher Tiefe" – Smart Contracts als interdisziplinäres Problem', *Jusletter* IT, 22 February 2018, 6; Riikka Koulu, 'Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement', (2016) 13 *SRIPTed*, accessed 9 February 2018 at https://script-ed.org/article/blockchains-and-online-dispute-resolution-smart-contracts-as-an-alternative-to-enforcement, 54; Olivier and Jaccard (supra n 46), 4; Weber (supra n 61), 3; Glarner and Meyer (supra n 68), 11; Michael Martin Kianička, *Die Agentenerklärung Elektronische Willenserklärung und künstliche Intelligenz als Anwendungsfall der Rechtsscheinhaftung* (Schulthess Juristische Medien, 2012), 53–9; Yves Poullet, 'La conclusion du contrat par un agent électronique' in *Commerce électronique – Le temps des certitudes* (Bruylant, 2000), 129–46.

international law are not suited to the intangible and ubiquitous environment of the blockchain whenever their application makes it necessary to establish the physical location of the blockchain transaction. This creates a lack of predictability as to the applicable law, and significant legal uncertainty.

The blockchain calls the traditional approach of private international law into question, since in reality it is impossible to establish the geographical location of blockchain transactions.[71] The blockchain is distinguished by its decentralised, network-based architecture. Transactions are incorporated in a block which forms part of the blockchain, of which every node (i.e., 'full node') in the network has an identical copy. This results in the distribution of data between network participants. In this kind of resource-sharing system, the involvement of a node is random and no one node has control over the other nodes in the network. In other words, transactions made using this technology are located everywhere and nowhere. There is not even a central server that could be used as an anchor to establish the location of the data.[72] The limits of the traditional rules of private international law, which seek to establish the physical location of the property or legal relationship, become swiftly apparent in the context of a private international law reasoning. It must therefore be admitted that the geographical location of blockchain transactions is of no importance: only conflict-of-law rules that are independent of any location criterion are able to provide a satisfactory connection to a national legal order.

While the technique of locating the legal relationship cannot be satisfactorily transposed into a virtual environment, it is possible to get around the difficulty of establishing the location by selecting the applicable law via a choice of law clause. However, this requires each of the parties to be able to effectively give his or her consent for the application of a certain law. In this regard, it must be noted that the use of a blockchain occurs within a network that is

---

[71] Same opinion: Graham-Siegenthaler and Furrer (supra n 47), 9 ('The blockchain has no such "closest connection" to any jurisdiction worldwide.'); Melanie Dulong de Rosnay, 'Peer-to-Peer as a Design Principle for Law: Distribute the Law', *Journal of Peer Production* (January 2015), Issue 6, accessed 9 February 2018 at http://peerproduction.net/issues/issue-6-disruption-and-the-law/peer-reviewed-articles/peer-to-peer-as-a-design-principle-for-law-distribute-the-law ('Distributed architectures fragment data and actions, thus challenging the localised rights model where each object or right can be assigned to one actor. The problem comes from the fact that peer-to-peer architectures aggregate and distribute technically insignificant fragments, while the law allocates rights and responsibilities to individual persons').

[72] In any case, locating the data at the place of the server is not a satisfactory solution, because this place is difficult to predict and can be easily manipulated. Same opinion: Dan Jerker B. Svantesson, *Private International Law and the Internet* (3rd edn., Kluwer Law International, 2016), 469. See e.g., CJEU, Case C-523/10, *Wintersteiger AG v Products 4U Sondermaschinenbau GmbH* (19 April 2012).

more 'closed' than mere Internet use. The blockchain is a digital peer-to-peer network, which implies a community aspect. This distinctive feature may influence the development of a new method of private international law that abandons any desperate attempt to locate blockchain transactions in the real world. The adoption of private international law rules designed specifically for legal relationships formalised via the blockchain would have the benefit of offering a simple means of achieving the objective of predictability of law and the resulting legal security.

V PROPOSALS FOR THE ADOPTION OF SPECIFIC PRIVATE INTERNATIONAL LAW RULES

Since the traditional approach of private international law is antithetical to the essence of the blockchain, it is necessary to seek a new method that takes the characteristics of this technology into account in order to connect blockchain transactions to a legal order.

Ideally, every State should apply the same rules of private international law, as this would enable genuine legal security. This level of uniformisation can only be obtained via an international instrument ratified by all States. Until this (utopian) result comes to pass, certain ideas can be gathered for the purpose of developing rules of private international law that take the specific features of the blockchain into account.

However, while the use of private international law rules provides a degree of predictability as to the applicable law, there remains the problem that each State's rules of substantive law will be different. The question is therefore whether the involvement of States is desirable or whether it would be preferable to allow self-regulation of the blockchain to develop.

V.A Rise of a *Lex Cryptographia*

Assuming that all blockchain transactions are international by nature, one may question whether it is really suitable to leave the various States with the task of determining the legal regime for these transactions in their territory. The intervention of States to establish a legal framework for the blockchain also seems unnatural if one considers the ideological foundations of this technology. The bitcoin blockchain model is community-based and even potentially offers an alternative approach to the economy. It demonstrates a firm desire to offer an economic model involving no financial intermediaries and no intervention by States. This model aspires to a system that provides the necessary security for international commercial operations without any involvement of the law or its actors. It therefore appears paradoxical to seek out legal rules to provide legal security in a system that is designed not to require this type of security.

The blockchain is fundamentally reliant on the paradigm of trust in the system.[73] This trust is placed not in a financial intermediary giving the impression of security, nor in a State acting as guarantor, but rather in a computer protocol that operates without human intervention once launched and which is impossible to stop. Users are thus at the mercy of a computer program in which they agree to place their trust without fully understanding the technology. The 'distributed trust' of all the members of the community of users provides the necessary security to ensure the sustainability of the system. This trust is not only placed in the computer protocol, but also in the other participants in the system. Blockchain technology effectively relies on a collective commitment, on the exchange and pooling of individual resources. Although the level of commitment may vary from one user to the other,[74] entering the system means participating in the system. Each blockchain consists in fact of a community of participants much more than of a community of users.

It therefore seems in keeping with the community-based spirit of the blockchain to allow the development of self-regulation. Purists will object that the system guarantees 100 per cent reliability. There is no risk provided that the computer executes the code in accordance with the instructions it contains. From this perspective, the code is sufficient to ensure the required security. The computer environment should therefore be sufficient, without requiring any legal instruments to function. But from the point of view of a legal expert, the lack of risk cannot be 100 per cent guaranteed and the system must therefore be controlled by a minimum number of rules to ensure that it functions correctly and will survive in the event of a malfunction. There is a real risk of a coding error, or of code being executed in a manner that does not correspond to the expectations or wishes of the parties.[75]

If the blockchain were to be self-regulated, with no intervention by State powers, it is plausible that the legal rules would be defined by the community of participants.[76] The consent of the participants in the blockchain is an essential condition for any attempted standardisation. Since the blockchain is a community of persons who reject any idea of centralisation and accept deci-

---

[73] See Alexandre Mallard, Cécile Méadal and Francesca Musiani, 'The Paradoxes of Distributed Trust: Peer-to-Peer Architecture and User Confidence in Bitcoin', *Journal of Peer Production* (January 2014), No. 4, accessed 9 February 2018 at http://peerproduction.net/issues/issue-4-value-and-currency/peer-reviewed-articles/the-paradoxes-of-distributed-trust.

[74] Some users develop the protocol, others validate the transactions, while others only make transactions.

[75] See Section IV.A.2.

[76] Or 'community of peers' in the terminology of de Rosnay (supra n 71). The concept of community of peers may be defined as a 'non-stabilised, evolving, or non-formalised group sharing a common interest or an ad hoc production purpose'.

sions taken by the majority, it seems appropriate to entrust participants with the task of defining rules that are suited to their protection requirements.[77] These rules must nonetheless correspond to the expectations of a large majority of users, as the legal rule must be the result of a consensus.[78] This set of legal norms not based on any legal system will draw their legitimacy from the fact that they are recognised by the community of participants in the blockchain. These anational legal rules will consist of the practices and customs of participants in the blockchain – in a sense, the general principles of the blockchain. The emergence of a *lex numerica*[79] – or more precisely a *lex cryptographia*[80] – will enable the formation of a legal environment that is detached from the legal environment of States. This would be in keeping with the original philosophy of the blockchain. The establishment of this kind of anational legal system requires confidence in the ability of participants in the blockchain to self-organise.

But simply adopting the rules is not sufficient: it is also necessary to establish a mechanism to monitor the application of those rules. The application of *lex cryptographia* must be monitored using a mechanism that corresponds to the logic underpinning the system, i.e. an online dispute resolution (ODR).[81] The dispute management role could be assigned to all members of the community – or to a body composed of members elected by the participants – which could be called into action in order to solve the dispute either on a consultative basis or by a decision adopted by vote. This 'peer judgement' mechanism would be perfectly compatible with the community spirit of a peer-to-peer network. It appears inevitable to us that participants in the blockchain will be granted the right to participate, in one way or another, in decision-making power as part of a public blockchain model. On the other hand, in a private or

---

[77] See Simon de Charentenay, 'Blockchain et Droit: Code is deeply Law', accessed 9 February 2018 at https://blockchainfrance.net/2017/09/19/blockchain-et-droit.

[78] See e.g., Jean-François Perrin, *Sociologie empirique du droit* (Helbing and Lichtenhahn, 1997), 31 ('law is the set of precepts which are said and recognised as right within a group' (translation from the original French)).

[79] In the terminology of Klaus Peter Berger, *The Creeping Codification of the New Lex Mercatoria* (2nd edn., Kluwer Law International, 2010), 290 (with further references). The idea of a *lex numerica* applicable to all online transactions has many similarities to the *lex mercatoria*, which can be applied to international business transactions.

[80] The term '*lex cryptographia*' is borrowed from Wright and De Filippi (supra n 25).

[81] See e.g., Gabrielle Kaufmann-Kohler and Thomas Schultz, *Online Dispute Resolution: Challenges for Contemporary Justice* (Kluwer Law International, 2004); Rinaldo Sali, 'Online Dispute Resolution (ODR): Crossing Technology and Disputes', in Andrea Schulz (ed.), *Legal Aspects of an E-Commerce Transaction* (Sellier, 2006), 249–59.

semi-private blockchain model, this dispute management role could also be assigned to the operator of the blockchain.

An extra step could even be taken by devising a computer dispute resolution (CDR), which could be called into action, or which would be triggered automatically in the event of a system malfunction.[82] It would then be necessary to implement a system to 'codify' the rules, i.e. to transcribe legal rules into computer codes ('law is code').[83] Where the terms of the dispute can be defined in a simple way, it might even be possible to encode them in a smart contract.[84] For example, the parties to a smart contract that has encountered problems relating to its execution on the blockchain could draw up a new smart contract to resolve their dispute, stating that the blockchain transaction will be executed in favour of the party proven right by the computer verification of data.

The establishment of an ODR would not only conform to the foundations of the blockchain by entrusting the verification of the elements relevant to the dispute either to participants in the blockchain or to a computer program, but also to its objectives by enabling 'decisions' to be rendered rapidly and at low cost. Clearly, execution of the decisions would also have to be made without any intervention by State powers, by means of measures that could be implemented on the blockchain itself.[85] Sanctions, or rather incentives, for the losing party to voluntarily comply could be considered if necessary.[86]

The development of a *lex cryptographia* combined with a CDR is probably the most suitable model of rules of law for open-access public blockchains that are managed by all their participants. However, determining the exact content of the *lex cryptographia* may prove to be difficult. Also, one must bear in mind the fact that rules of law transcribed into computer codes are not flexible

---

[82] See Koulu (supra n 70); Weber (supra n 61), 11–13.

[83] Primavera De Filippi and Samer Hassan, 'Blockchain Technology as a Regulatory Technology: From Code Is Law to Law Is Code' (5 December 2016), 21(12) *First Monday*, accessed 9 February 2018 at http://firstmonday.org/ojs/index.php/fm/article/view/7113/5657#author; S.I. Lex, 'Comment "Code Is Law" s'est renversé en "Law Is Code"' (24 January 2014), accessed 9 February 2018 at https://scinfolex.com/2014/01/24/comment-code-is-law-sest-renverse-en-law-is-code.

[84] See Koulu (supra n 70), 40–69. This author examines the possibility of using a smart contract as a means of conflict resolution by exploring the possibilities of development in this direction.

[85] For example, one could consider setting up a mechanism that would force users to provide their private key when entering a conflict resolution process, so that the transfer of cryptocurrencies from one wallet to the other could be carried out in accordance with the 'decision'. Other less intrusive means could also be investigated, such as escrow smart contracts. See Glarner and Meyer (supra n 68).

[86] For example, lowering the offender's e-reputation or prohibiting access to the blockchain could be effective sanctions. See Kaufmann-Kohler and Schultz (supra n 81), 223–33; Koulu (supra n 70), 44–7; de Charentenay (supra n 77).

enough to take into consideration the details of a given situation.[87] Private or semi-private blockchains could resolve this difficulty by establishing rules – for example, on the model of a membership agreement or general terms and conditions – to which each participant must sign up in order to access the network. These rules may consist of rules specific to the blockchain they regulate, or refer to the *lex cryptographia*.

V.B Creation of a New Category of Law

Even if blockchain participants manage to implement self-regulation of the system, this will not prevent blockchain transactions from interacting with law rules applicable in the real world.[88] For example, when the repayment of a loan is triggered automatically on the blockchain on the agreed deadline, but the borrower is bankrupt, the blockchain transaction enters into conflict with the mandatory law rules for insolvency proceedings. The fact that a transaction can no longer be modified once it is recorded in a block of the blockchain poses a risk when the transaction cannot take place due to circumstances that have occurred in the real world.[89] This example shows that it is necessary to create a legal bridge between the virtual world and the real world.

Private international law fulfils precisely this role of a bridge between legal orders. Given that the private international law rule will create a link between the virtual world (i.e., the technological order of the blockchain) and the real world (i.e., the legal order of a State), it seems to us that this link should be positioned in the centre of the private international law rule. This approach provides a solution to the inherent difficulty of the lack of a location for blockchain transactions.

On this basis, we will examine which private international law rules could be adapted to this technology.

V.B.1 Recognition of blockchain transactions

The application of private international law rules enables blockchain transactions to be connected to a national legal order. The objective is to provide these transactions with the legal framework, and therefore the legal force, that they are deprived of as long as they take place outside any State legal system. The private international law rules must therefore enable blockchain transactions

---

[87] See De Filippi and Hassan (supra n 83).

[88] See Svantesson (supra n 72), 2–3.

[89] See Mik (supra n 34), 283 ('self enforcement may deprive contractual relationships of their adaptability and preclude the parties from adjusting their legal and commercial positions in response to changed circumstances').

to be connected to a State which has agreed to grant them legal effects by recognising their legal existence.

If a State refuses to consider these transactions legally binding, for example because it finds them to be incompatible with its public policy, the connection to this legal order will have no legal scope. It is therefore necessary for the State whose authorities are concerned by a blockchain transaction to recognise – at least implicitly – transactions carried out on the blockchain. This recognition can be achieved by creating a new category of law devoted to legal relationships formalised via the blockchain or on the Internet in general.

V.B.2 Jurisdiction

If a State recognises the legal existence of blockchain transactions, it is possible to institute proceedings in its courts. A case can only be submitted to a State's courts if the legal order of the State considers that blockchain transactions are legally binding. Of course, this approach presumes that the defendant can be identified, which may pose a problem in practice. The two issues are connected, insofar as it is unlikely that a judge will consider a blockchain transaction to have legally binding effects if it is not possible to identify the other contracting party. Further, a State will only grant the protection of its courts if the decision they render can be enforced. As it is doubtful that the authorities of a State will be able to enforce the decision directly on the blockchain, the decisions rendered by State courts can concern persons only. If these difficulties can be overcome, the first question is whether a State accepts the jurisdiction of its authorities to rule on actions relating to this type of transaction.

The most simple solution is to allow the possibility of a choice of court agreement. If the participants in a blockchain are able to agree on the choice of court in the event of a dispute arising in connection with participation in a blockchain, this solution must be preferred. For example, the prorogation of jurisdiction may be stated in the base contract that is 'backed up' by the smart contract, or even directly in the smart contract. The choice of court can also be specified in the rules that must be accepted by any participant to gain access to a private or semi-private blockchain. For example, the choice of court may be stated in the general terms and conditions for the blockchain.

If the designated court is in Switzerland, the question to be settled by a Swiss court is whether the written form has been adhered to.[90] If the Lugano Convention is applicable, the prorogation of jurisdiction shall also be in

[90] Art. 5(1), 2nd sentence, SPILA states that: 'The agreement may be entered into in writing, by telegram, telex, telecopier or any other means of communication which permits it to be evidenced by a text.'

writing or evidenced to writing.[91] The Convention states that any communication by electronic means which provides a durable record of the agreement shall be equivalent in writing.[92] A prorogation of jurisdiction specified in the general terms and conditions applicable to a contract entered into electronically, and which have been accepted via a click, meets the criteria for a written form if it is possible to save and print the general terms and conditions before entering into the contract.[93] The important element is that the agreement of the parties as to the choice of court can be effectively established. The Lugano Convention also provides that the choice of court agreement can be in a form which accords with practices which the parties have established between themselves and, in international trade or commerce, in a form which accords with a usage of which the parties are or ought to have been aware and which in such trade or commerce is widely known to, and regularly observed by, parties to contracts of the type involved in the particular trade or commerce concerned.[94] However, we believe it is premature to claim that there are already practices or a usage in relation to the blockchain. If either of the parties can be defined as a consumer, the scope of the choice of court agreement is reduced in order to protect the consumer.[95]

In States that have ratified it,[96] the Hague Convention on Choice of Court Agreements is applied to determine the validity of a choice of court agreement in relation to its scope of application.[97] The Convention also requires that a choice of court agreement must be concluded or documented in writing or by any other means of communication which renders information accessible so as to be usable for subsequent reference.[98]

---

[91] Art. 23(1)(a) of the Lugano Convention (see also Art. 1 of the Lugano Convention). This Convention is applicable if one or more of the parties is domiciled in a State bound by the Convention. Given this requirement, the application of the Lugano Convention will only be possible in a private and semi-private blockchain model where all participants are domiciled in a Contracting State.

[92] Art. 23(2) of the Lugano Convention.

[93] CJEU, Case C-322/14, *Jaouad El Majdoub v CarsOnTheWeb.Deutschland GmbH* (21 May 2015).

[94] Art. 23(1)(b) and (c) of the Lugano Convention.

[95] Art. 114(2) SPILA; Art. 17 of the Lugano Convention.

[96] To date, the Member States of the European Union, Mexico, and Singapore are applying the Hague Choice of Court Agreements Convention.

[97] Arts 1 and 2 of the Hague Choice of Court Agreements Convention. It should be noted that this Convention does not apply when one of the parties is a consumer (Art. 2(1)(a)).

[98] Art. 3(b) of the Hague Choice of Court Agreements Convention. See Andrea Schulz, 'The Hague Conference Project for a Global Convention on Jurisdiction, Recognition and Enforcement in Civil and Commercial Matters (the Hague Judgments Project), Electronic Commerce and Intellectual Property', in Andrea Schulz (ed.), *Legal Aspects of an E-Commerce Transaction* (Sellier, 2006), 293–308 ('This text …

Where it is not possible to agree on the choice of court, which in principle is the case for public blockchains where it is difficult to identify the participants, it is the responsibility of each State to define the situations in which it intends to grant the protection of its courts to the participants in a blockchain. The question arises in a more general manner with actions in tort where the agreement of the parties on the choice of court is difficult to obtain. In Switzerland, for example, Swiss courts in the domicile or, in the absence of domicile, in the habitual residence of the defendant have general jurisdiction. Furthermore, Swiss courts at the defendant's place of business also have jurisdiction to entertain actions arising out of the operations of such place of business. But these general rules do not appear sufficient, in particular since the defendant will not always be immediately identifiable. In our view, the jurisdiction of the Swiss courts must be extended to other situations. But we have seen that any attempted connection based on aspects or effects of the blockchain is bound to fail, since it is impossible to establish the location of blockchain transactions.[99] On the other hand, it is possible to establish the jurisdiction of the Swiss courts at the domicile or habitual residence of the claimant. Swiss private international law already specifies this forum for actions brought by consumers.[100]

A State's adoption of rules clearly establishing the international situations in which it grants the protection of its courts makes it possible to predict which forum should be used to resolve disputes. Knowing the forum in advance also means being able to anticipate the applicable law, since the court to which the case is referred will apply the conflict-of-law rules of its State in order to determine the law applicable to the legal relationship. This enables a considerable improvement in legal security.

V.B.3 Choice of law

Once the authorities of a State have acknowledged their jurisdiction, they must determine the law applicable to blockchain transactions. As with jurisdiction, the most simple solution is to allow the possibility of a choice of law agree-

---

should be sufficient to enable the Convention to deal with the validity of choice of court agreements concluded by electronic means of communication yet to be developed', at 300).

[99] See section IV.B. In our opinion, the criterion of accessibility to the website in the State of the forum, which is used by the CJEU with regard to torts, is not suitable for blockchain transactions. See e.g., CJEU, Cases C-509/09 and C-161/10, *eDate Advertising GmbH and Others v X and Société MGN Limited* (25 October 2011); CJEU, Case C-441/13, *Pez Hejduk v EnergieAgentur.NRW GmbH* (22 January 2015).

[100] Art. 114(1)(a) SPILA; Art. 16(1) of the Lugano Convention.

ment.[101] The chosen law must be that of a State that recognises blockchain transactions, so that they can have a legally binding effect.

The choice of law may complement a choice of court agreement and also be agreed upon in the base contract that is 'backed up' by the smart contract, in the smart contract itself, or in the general terms and conditions of the blockchain. The choice of law by the parties makes it possible to obtain the necessary degree of legal security. The parties to a smart contract, for example, need to know which law governs their legal relationship in order to avoid later facing unexpected legal conditions rendering the contract unlawful or impossible to execute.

The qnestion is which fallback rule can be provided in the event that no valid choice of law is made. Attempting to establish such a rule again comes up against the intrinsic impossibility of establishing the geographical location of blockchain transactions. In any case, it is not possible to apply a connecting factor that seeks to determine the State with which the issue has the closest connection. In our view, the only option is to provide, in such cases, for the application of *lex fori*.[102] Any other attempt to establish an objective connection with a State appears bound to fail. In this regard, it is significant that the Monegasque drafters of a proposed act suggested that Monegasque law should apply whenever the blockchain transaction produces effects within the territory of the Principality of Monaco.[103] This rule does not seek to establish the location of the transaction, but simply to apply *lex fori* whenever there is a connection of any kind with the forum in question. This example clearly demonstrates that the issue arises more at the level of determining the jurisdiction of the authorities than at that of the applicable law.

The difficulty of establishing a connection has been posed in very similar terms in relation to determining the law applicable to securities held with an intermediary. The adoption of the Hague Convention on the Law Applicable to Certain Rights in Respect of Securities held with an intermediary[104] has made

---

[101] It should be noted that even if the Hague Principles on Choice of Law in International Commercial Contracts do not take into account the particularities of Internet contracts and in particular blockchain transactions, these Principles may be useful for examining the validity of a choice of law clause within their application scope. These Principles only apply if each party to the contract is acting in the exercise of its trade or profession, which in particular excludes consumer contracts (Art. 1(1)).

[102] Graham-Siegenthaler and Furrer (supra n 47), at 9, also conclude that the application of the law of the forum is inevitable in view of the fact that '[t]he closest connecting factor test must inadvertently fail'.

[103] See draft Art. 5 of the Proposal for a Blockchain Act ('*Proposition de loi relative à la blockchain*' (see supra n 33)).

[104] This Convention, which entered into force on 1 April 2017, has been applied in Switzerland since 1 January 2010 (SR 0.221.556.1; see AS 2009 6579; BBl 2006 8817).

it possible to formalise uniform conflict-of-law rules that, in particular, are adapted to the specific issues raised by the dematerialisation of securities.[105] This is the first international instrument to take into account the aspects of private international law on the trading of securities in a dematerialised environment. This Convention favours the choice of law as a primary rule.[106] It only provides for an objective connection to the law of the State where the direct intermediary of the account holder maintains his or her securities account[107] as a fallback rule when no valid choice of law is made. The fallback rule should only be applied in very exceptional cases, since the parties to a disposition of intermediated securities are known and each investor is connected to an intermediary via an account agreement in which a choice of law can easily be provided. These two aspects are fundamentally different in the blockchain environment. As we have seen, any connection to the location of the user's account is too superficial and random, as it implies establishing the location of his or her private key.[108] While it is difficult in practice to determine the location of a securities account held with an intermediary, it is even more difficult to establish the location of a digital wallet. In these circumstances, it is difficult to find any other objective connection than the *lex fori*.

A distinctive feature of the Hague Securities Convention is that it provides for the designated law to apply not only to the parties to the account agreement governing the account to which the security has been credited, but also to the rights of third parties to the same security.[109] In particular, this law determines the order of priority between several creditors. The rights of third parties are protected in two cases: when the parties to the account agreement decide to change the applicable law, and in the event of insolvency proceedings.[110] This rule could be used for blockchain transactions by specifying that the designated law may be asserted against third parties, while allowing for an exception when the parties change the law designated in the choice of law agreement and when insolvency proceedings are brought against one of the participants in the blockchain.

The Hague Securities Convention is in force today in Switzerland, the United States of America, and Mauritius.

[105] Art. 1(1)(a) of the Hague Securities Convention. The term 'securities' includes all financial instruments or assets (other than cash).

[106] Art. 4 of the Hague Securities Convention.

[107] This rule is referred to as 'Place of the Relevant Intermediary Approach' or 'PRIMA'. See Art. 5 of the Hague Securities Convention.

[108] See section IV.A.

[109] See Art. 2(1) of the Hague Securities Convention.

[110] See Arts 7 and 8 of the Hague Securities Convention.

A conflict-of-law system that provides for the application of the chosen law as a primary rule, and of *lex fori* as a fallback rule, appears fairly easy to implement for private and semi-private blockchains. These blockchains are administrated by operators who have duties typical of intermediaries[111] and are therefore able to link access rights to the blockchain with acceptance of the rules and in particular a choice of law agreement. But the chosen law, which will be the same for all participants in the blockchain, might conflict with the consumer protection rules.[112] On the other hand, choice of law appears more difficult to implement for public blockchains, where there is no equivalent of a central administering authority. The same applies in the event of a tort, in which it is more difficult to obtain the agreement of the tortfeasor as to the applicable law, supposing that he or she can be identified. If it is not possible for the parties to agree on the applicable law, application of *lex fori* seems inevitable when the dispute is brought before the State courts.

A State's adoption of rules enabling the clear establishment of the applicable law guarantees a minimum degree of legal security. Party autonomy should be promoted in order to take into account the desire for individual freedom held dear by the blockchain users. Translated into concepts of private international law, this means leaving as much room as possible for choice of law and choice of court agreement.

V.B.4 Recognition and enforcement of foreign judgments

As for the rules on the recognition and enforcement of foreign judgments, it is the responsibility of each State to define the conditions under which it agrees that foreign decisions will be legally binding within its territory. Swiss private international law states that a foreign decision shall be recognised and shall be declared enforceable in Switzerland if the authorities of the State where the decision was rendered had jurisdiction, if the decision is final or no longer subject to any ordinary appeal, and if such decision is not incompatible with Swiss public policy.[113] If the Lugano Convention is applicable and the decision was rendered in another Contracting State, it will be recognised and declared enforceable essentially on the condition that the decision is not contrary to public policy in the State in which recognition is sought.[114]

---

[111] See Teresa Rodríguez-de-las-Heras Ballell, 'Rules for Electronic Platforms: The Role Of Platforms and Intermediaries in Digital Economy – A Case for Harmonization', 11–13, accessed 9 February 2018 at http://www.uncitral.org/pdf/english/congress/Papers_for_Programme/139-RODRIGUEZ-Rules_for_Electronic_Platforms.pdf.

[112] The consumer protection rules may limit or exclude the possibility of making a choice of law. See e.g., Art. 120(2) SPILA ('No choice of law is allowed').

[113] See Arts 25 to 29 SPILA.

[114] See Arts 32 to 56 of the Lugano Convention.

It is important for a State to clearly define the conditions under which it agrees that a foreign decision will be legally binding within its territory. The possibility of obtaining the recognition and enforcement of the foreign decision, for example in the State of the defendant's domicile, is a criterion that must be taken into consideration when choosing the court.[115]

VI CONCLUSION

Private international law resolves the difficulty resulting from the apparent incompatibility between the transnationality of the Internet and the national character of private law by connecting to a State legal relationships that are free of any territorial connection. But the ubiquitous and dematerialised nature of the Internet makes it difficult to apply traditional conflict-of-law rules and leads to an often unpredictable result. Further, connecting a legal relationship to a State can seem artificial when it originates from the Internet.

The specific characteristics of the Internet must be taken into account in order to adapt the connecting factors used in private international law, or to seek out new connecting factors, or even to establish a new method for connecting a legal relationship to a legal order. This approach must be able to accommodate all technologies using the Internet, as the problem of connection is fundamentally the same regardless of the technology used.

The blockchain provides an opportunity for development in this area, since it is an example of a technology with which no location can be established. Further, this technology enables legal relationships to be formalised not only without the parties knowing each other but also without any human involvement. Electronic agents are on the rise: transactions must be expected to be concluded and executed autonomously within the network of the Internet.

Each State must determine whether or not it recognises the legal effects of relationships formalised over the Internet, in particular via the blockchain. The rules on international jurisdiction are of paramount importance, since they determine the situations in which a State will offer the protection of its courts. In particular, they determine whether a court chosen by the parties is required to settle the dispute. The rules of jurisdiction should be combined with an adapted private law framework, in particular in the area of contract and tort, because in the absence of a valid choice of law the application of *lex fori* is the only solution in this area.

---

[115] The future Hague Convention on the Recognition and Enforcement of Foreign Judgments will facilitate the recognition and enforcement of decisions between contracting States. See https://www.hcch.net/en/projects/legislative-projects/judgments accessed 9 February 2018.

Published by
Edward Elgar Publishing Limited
The Lypiatts
15 Lansdown Road
Cheltenham
Glos GL50 2JA
UK

Edward Elgar Publishing, Inc.
William Pratt House
9 Dewey Court
Northampton
Massachusetts 01060
USA

A catalogue record for this book
is available from the British Library

Library of Congress Control Number: 2018967803

This book is available electronically in the Elgaronline
Law subject collection
DOI 10.4337/9781788115131

ISBN 978 1 78811 512 4 (cased)
ISBN 978 1 78811 513 1 (eBook)

Printed and bound in Great Britain by TJ International Ltd, Padstow

EE
Elgar

EDITED BY

Daniel Kraus, Thierry Obrist
and Olivier Hari

Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law