HCCH

Connecter Protéger Coopérer Depuis 1893
Connecting Protecting Cooperating Since 1893

HCCH a|Bridged Edition 2019

The HCCH Service Convention in the Era of Electronic and Information Technology

11 December 2019
The Hague
(Netherlands)

Hague **C**onference on Private International Law – **C**onférence de La **H**aye de droit international privé

HCCH a|Bridged
Edition 2019:

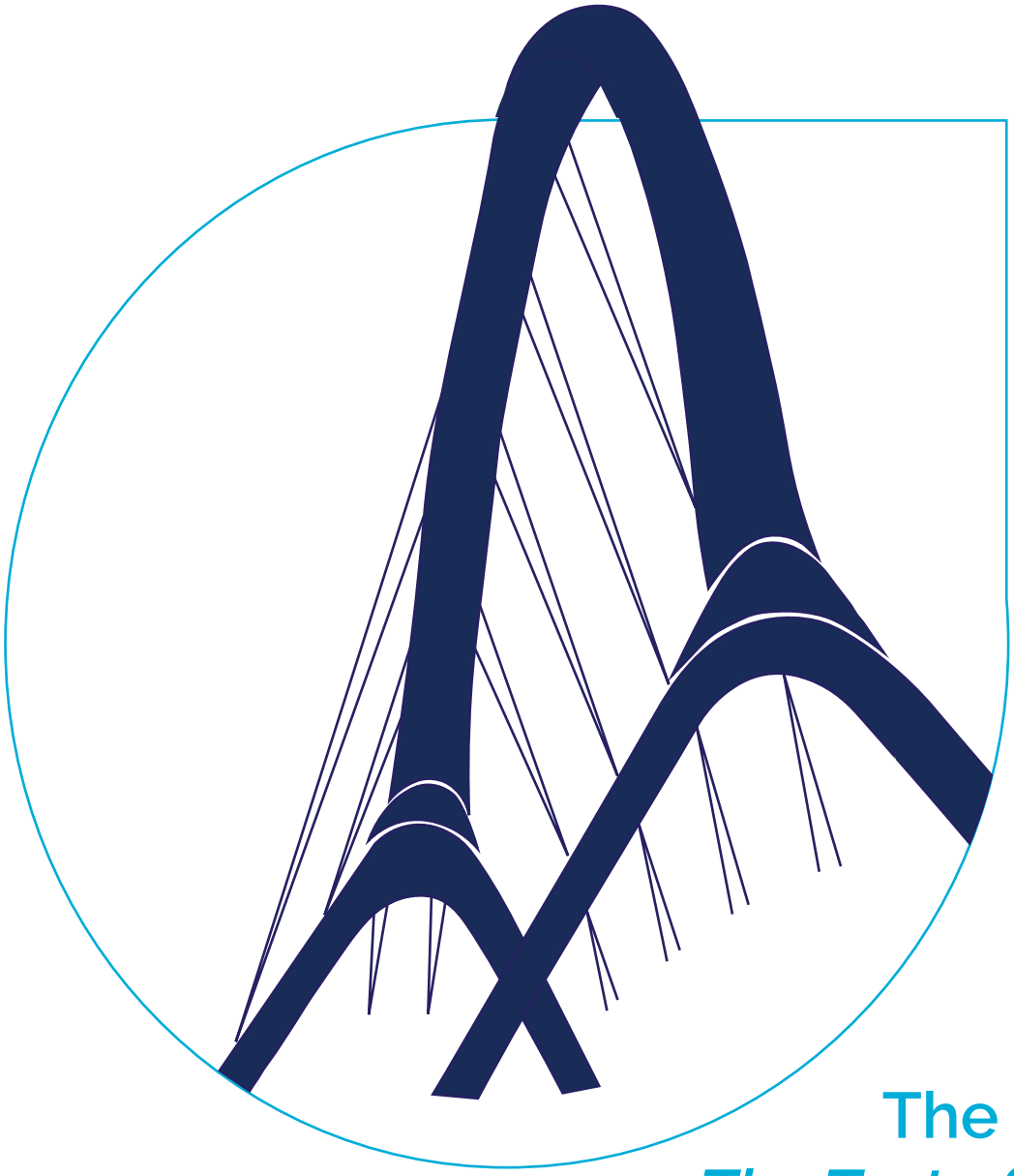
The HCCH Service Convention in the Era of Electronic and Information Technology

Published by
The Hague Conference on Private International Law – HCCH
Permanent Bureau
Churchillplein 6b
2517 JW The Hague
Netherlands

+31 70 363 3303
+31 70 360 4867
secretariat@hcch.net
www.hcch.net

Published in The Hague, the Netherlands

TABLE OF CONTENTS



The Open Lab:
The Text of Tomorrow

This section is an academic examination of the HCCH Service Convention and how it will operate in the world of tomorrow.

LAUNCHING THE HCCH SERVICE CONVENTION INTO THE CRYPTO SPACE

BY FLORENCE GUILLAUME, PROFESSOR OF PRIVATE INTERNATIONAL LAW, UNIVERSITY OF NEUCHÂTEL, SWITZERLAND
AND
SVEN RIVA, PH.D. STUDENT IN PRIVATE INTERNATIONAL LAW, UNIVERSITY OF NEUCHÂTEL, SWITZERLAND

I. Service Convention and technology

The *Hague Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters* (the "Service Convention") has as its main objective the setting up of a system for transmission of documents for service abroad.[114] More specifically, the Service Convention aims: "a) to establish a system which, to the extent possible, brings actual notice of the document to be served to the recipient in sufficient time to enable him to defend himself; b) to simplify the method of transmission of these documents from the requesting State to the requested State; [and] c) to facilitate proof that service has been effected abroad, by means of certificates contained in a uniform model."[115] The Service Convention contains rules of international cooperation whose purpose is to facilitate the transmission of a document from one Contracting Party to another. It does not, however, deal with the way to serve the document to the addressee, as this is a matter of domestic law.

The Service Convention was conceived at a time when the international transmission of documents could only be made by postal mail. Nonetheless, it has the particularity of allowing the transmission of documents by any appropriate means, without providing any specific method for the transmission. The primary requirement is that the transmission of a document abroad must be made as soon as possible.

The operation of the Service Convention has been reconsidered in light of the technological developments that have occurred since its adoption, so as to incorporate the possibility to transmit documents by fax, and then by e-mail.[116] It was noted during a Special Commission meeting in 2003 that "the spirit and letter of the [Convention] do not constitute an obstacle to the usage of modern technology and that [its] application and operation can be further improved by relying on such technologies."[117] For this reason, "the operation of the Convention [is] to be considered in light of a business environment in which use of modern technology [is] now all pervasive, and that the electronic transmission of judicial communications is a growing part of that environment."[118] The Special Commission concluded that "the transmission of documents internationally for the purposes of the Convention can and should be undertaken by IT-Business methods including e-mail."[119] It was thus recognized that the use of the Internet could facilitate the transmission of

114 HCCH, *Practical Handbook on the Operation of the Service Convention*, The Hague, 2016 (the "Practical Handbook"), No 9.

115 *Ibid.*, No 6, with reference to V. Taborda Ferreira, "Rapport explicative", in *Actes et documents de la Dixième session (1964),* Tome III, *Notification*, The Hague, 1965, pp. 363 f.

116 See Practical Handbook (*op. cit.* note 114), Annex 8, Nos 1-9.

117 HCCH, Conclusions and recommendations adopted by the Special Commission on the practical operation of The Hague Apostille, Evidence and Service Conventions (28 October to 4 November 2003), October 2003 (the "Conclusions and recommendations 2003"), No 4.

118 *Ibid.*, No 59.

119 *Ibid.*, No 62.

information internationally and thereby the cooperation between the authorities of the Contracting Parties. This would greatly improve the overall operation of the Service Convention.

However, the Special Commission already noted in 2003, and again in 2009, that the use of e-mail, or even fax, for the transmission of documents abroad was not yet possible in all Contracting Parties.[120] It thus appears that the transition of the Service Convention to the technological environment is difficult to achieve in practice. The recent evolution of computer technology induced by blockchain technology could favor this transition by providing a digital environment that guarantees the security requirements necessary for the application of the Service Convention.[121]

The use of electronic means for the service of documents to the addressee is of course a desirable development. Whereas technologies such as e-mail or fax could greatly benefit the Service Convention by improving the speed of delivery and simplifying the process, blockchain technology would combine those advantages while providing increased security to the electronic service of documents to the addressee. In this paper, we will explore this possibility by examining whether the use of blockchain technology for the transmission of documents abroad could improve the practical operation of the Service Convention while guaranteeing sufficient security to the Contracting Parties to the Convention. The question of the actual process of transmission will not be elaborated in this paper.

After these introductory remarks about the use of technology in the context of the Service Convention (I), a brief description of blockchain technology will clarify the main features of this new technology (II). On this basis, we will then examine whether and how blockchain technology can be used for the service of documents abroad (III). We will conclude these first academic thoughts on the use of blockchain technology to improve the operation of the Service Convention with a few practical remarks (IV).

II. Blockchain technology in a nutshell

Since the compatibility of blockchain's architecture with the Service Convention will be examined, it is necessary to briefly review the basic characteristics of this technology.[122] The following observations will use the Bitcoin[123] model as a reference to describe the technical aspects of this technology. Bitcoin is a blockchain designed as a money transfer system that works with bitcoin, the most capitalized cryptocurrency. It should be noted that other blockchains may differ from this reference model on certain technical or conceptual points.

---

120 *Ibid*., No 64; HCCH, Conclusions and recommendations of the Special Commission on the practical operation of The Hague Apostille, Service, Taking of evidence and Access to justice Conventions (2 to 12 February 2009), February 2009 (the "Conclusions and recommendations 2009"), No 38.

121 Although security requirements should not be stricter than those currently existing for paper transmission: Practical Handbook (*op. cit*. note 114), Annex 8, No 14.

122 This Chapter is inspired from F. Guillaume, "L'effet disruptif des smart contracts et des DAOs sur le droit international privé", in A. Richa/ D. Canapa (eds), *Droit et économie numérique*, Lausanne 2020 (forthcoming).

123 Hereafter, "Bitcoin" will refer to the Bitcoin blockchain and "bitcoin" will refer to the bitcoin cryptocurrency. The same logic will be followed with other cryptocurrencies and their underlying blockchains.

a) Genesis of blockchain

Blockchain is presented by specialists as a technology that is driving a revolution on the Internet by enabling the creation of a new generation of distributed and cryptographically secure computer programs. Above all, this technology is at the origin of a new low-cost money transfer system, operating without financial intermediaries, and freely accessible from anywhere in the world and to anyone equipped with an electronic device connected to the Internet (e.g., a computer or a smartphone). Bitcoin[124] is the first publicly known use of blockchain technology. It serves as a large-scale international currency where money transfers take place on a cryptographically secure distributed ledger. Bitcoin has the particularity of being, so to speak, "issued" by blockchain technology. Unlike State-issued fiat currencies, no central regulatory authority has control over bitcoin and it is not legal tender. Therefore, the bitcoin rate cannot be controlled by a State authority (e.g., a central bank). Bitcoin has profoundly changed the financial ecosystem, which has led to blockchain being labeled as a "disruptive technology."[125]

Since the launch of Bitcoin in 2009,[126] many more blockchains have been released with their own cryptocurrencies. Ethereum was launched in 2015 and its ether is the second largest capitalized cryptocurrency.[127] Ethereum differs from Bitcoin in that it pursues a different objective than simply transferring money. This blockchain has been developed in order to facilitate the implementation of a second layer of programming that allows the transfers of cryptocurrencies to be automated. The possibility of introducing a computer program, referred to as a "smart contract,"[128] which, in particular, allows a transfer of cryptocurrencies to be made conditional on a series of rules, has opened up new perspectives for the use of blockchain technology. This kind of application has attracted the attention of lawyers, as smart contracts can be used in contractual matters as a means to perform the financial obligation provided for in a contract, or even to "digitalize" a contract or to create a "digital contract."[129]

b) Basics of blockchain

Blockchain is a distributed ledger technology.[130] This is a data management model in which transactions are recorded simultaneously on a great number of computers across the world. The network of computers is organized in a peer-to-peer fashion, which means that the registry containing all transactions is distributed to all computers in the network, removing the need for a centralized record or master copies. The computers are in constant communication and continuously share the state of the blockchain.

---

124 S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, available at: < https://bitcoin.org/bitcoin.pdf > (last consulted on 16 March 2020).

125 A. M. Antonopoulos, *The Internet of Money*, Vol. 1, 2016, Chapter 1: What is Bitcoin?

126 The first block of Bitcoin (the "genesis block") was created in January 2009.

127 V. Buterin, Ethereum White Paper – A Next Generation Smart Contract & Decentralized Application Platform, November 2013, available at: < https://www.blockchainresearchnetwork.org/wp-content/plugins/zotpress/lib/request/request.dl.php?api_user_id=2216205&dlkey=LIWF7NVA&content_type=application/pdf > (last consulted on 16 March 2020).

128 The term "smart contract" was coined by NICK SZABO, "Smart Contracts": Formalizing and Securing Relationships on Public Networks, First Monday, Vol. 2, 1st September 1997, available at: < http://firstmonday.org/article/view/548/469 > (last consulted on 16 March 2020).

129 See *e.g.*, F. Guillaume (*op. cit.* note 122), (forthcoming).

130 See *e.g.*, F. Guillaume, "Aspects of private international law related to blockchain transactions", in D. Kraus, T. Obrist and O. Hari (eds), *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law*, Cheltenham/Northampton, 2019, pp. 49-82, at pp. 54-56.

Blockchain is a decentralized technology entirely managed by the community of users who hold amounts of cryptocurrency. The fact that the network does not need to be managed by a central institution (e.g., a bank or any other financial intermediary) is a key feature of this technology. Unlike digital platforms such as Uber or Airbnb, blockchains can be managed independently without the intervention of an intermediary.

Blockchain works according to a system of distributed trust between users. Its use does not require trust to be placed in a central institution or in the other party to the transfer of cryptocurrencies. Each user can have a copy of the blockchain on his or her own computer and can thus check by himself or herself the validity of all the transactions carried out. The transaction register (i.e., the blockchain ledger) is indeed public. Bitcoin has introduced a paradigm shift in the financial ecosystem by transferring the trust that was placed in the central authorities (or trusted third parties) to the computer system itself.

Transactions are carried out through several stages of a decentralized consensus mechanism, which provides the trust necessary for the operation of the entire cryptocurrency transfer system.[131] The validity of a transaction is first verified by the computers on the network. They identify the accounts participating in the transaction on the basis of an electronic signature attached to each account, which is composed of a set of two cryptographic keys that guarantee the anonymity of the account holder.[132] The transaction is then integrated into a block of several transactions that are validated simultaneously by a computer or, more generally, a group of computers that have managed to find at random a sequence of digits that allows the system to validate the block. As soon as the block is validated, it is added to the chain and linked to the previous block so as to make up the chain of blocks constituting the transaction register. Computers validating transactions are referred to as "miners." They are paid both by the participants and by the system, which "issues" new units of bitcoin to pay for their work.

Within Bitcoin, all participants are treated equally. This blockchain is accessible to everyone and anyone can make transactions without being limited by State borders. The computers in the network can also be located anywhere. Bitcoin is not subject to any central authority, government, or central bank control. The network is censorship resistant as no one has the power to change the rules of the system or deny access to an individual. It is virtually impossible to exercise power or control over the Bitcoin blockchain, either by preventing transactions or by modifying transactions that have already taken place.[133] Once a transaction is recorded on the blockchain, it is time-stamped, tamper-proof, and cannot be corrupted nor deleted.[134]

---

131 There are several types of consensus mechanisms. Bitcoin uses Proof of Work (PoW), which is still the mechanism used by major blockchains.

132 Each Bitcoin user has (at least) one Bitcoin identity resulting from a set of two cryptographic keys. The person transferring bitcoin units must sign the transaction with his or her private key. The associated public key allows computers on the network to identify the user's account and to verify the validity of the transaction. The recipient's public key is embedded in the transaction so that, after it is added to a new block and validated by the minors, the recipient is able to retrieve the transferred units of bitcoin by using his or her own private key.

133 It should be noted, however, that a powerful miner (or several miners working together) can take control of Bitcoin by controlling 51% of the mining activity. The control of the mining activity would grant the power to block new transactions or double spend units of bitcoin. This attack, which is theoretically possible but considered unlikely, is referred to as the "51% attack". See K. Werbach, "Trust, But Verify: Why the Blockchain Needs the Law", *Berkeley Technology Law Journal* 2018, Vol. 33, pp. 489-552, at pp. 515-517.

134 See A. M. Antonopoulos (*op. cit.* note 125), Chapter 1.4; Legaler, Blockchain for Lawyers, 2018, available at: < https://www.legaler.com/wp-content/uploads/2018/12/Blockchain-for-Lawyers-eBook.pdf?utm_medium=email&utm_campaign=eBook%20Delivery&utm_content=eBook%20Delivery+&utm_s

c) Access to blockchain

The basic blockchain characteristics described above took Bitcoin as a reference model. This blockchain is a permissionless computer network, meaning that anyone can access it to make transactions at any time and from any location, without the need for permission. Bitcoin is also open source, which means that anyone has access to its software code and any computer developer can make improvement proposals to the network[135] or reproduce the software code to run a new blockchain. Ethereum, as well as many other blockchains, are similar open networks.

Some blockchains deviate from this reference model by being managed by a central authority. This type of blockchain is usually developed by a State, a company or a bank, which retains control over the system and manages access rights. These permissioned blockchains are not open networks: access is subject to authorization and the code is usually not open source.[136] An example is the (future) blockchain Libra from Facebook.

Unlike permissionless blockchains, which guarantee (at least in theory) the anonymity of users, permissioned blockchains typically require users to provide identification. Furthermore, this blockchain model is not censorship resistant as the system is controlled by a central authority. Moreover, unlike the Bitcoin reference model that has been deployed internationally, permissioned blockchains can be bounded by State borders. For example, the central authority can allow access to the blockchain only to persons residing in a particular State. This model usually limits the number of computers in the network, in particular the number of miners, and restricts their location within the territory of one single State. When the nodes running a blockchain are contained within the borders of a single State, the security of the whole network is compromised. The integrity of a permissioned blockchain may be completely at risk, for example, when the State in which the nodes are located declares any use of a blockchain illegal in order to preserve its national economy, prohibits mining activity for environmental reasons, or orders a general shutdown of the Internet[137] due to disturbances on its territory. Permissioned blockchains offer, paradoxically, a lower level of security than permissionless blockchains.

There is a fundamental conceptual difference between permissionless and permissioned blockchains. The launch of Bitcoin is part of an ideology that sees blockchain technology as a means of freeing oneself from the power of States and financial intermediaries.[138] The initial objective was to create the foundations for a new, self-sustaining economic model, by setting up a payments system (Bitcoin) over which governments and central banks could not exercise control. By reintroducing a trusted third party into the system, permissioned blockchains create an environment that loses its open access and neutrality, presents a risk of censorship, is not public, and is not necessarily cross-border. The more nodes exist in the network and the more decentralized the power over the network is, the safer a blockchain can be considered. Permissionless blockchains

ource=CM&utm_term=Click%20Here%20to%20Download%20eBook > (last consulted on 16 March 2020), p. 11; WERBACH (note 133), pp. 523 f.

135 Program updates are done by Bitcoin Improvement Proposal.

136 It is, of course, also possible to launch "mixed", partially open blockchains, for example by providing an authorization system to access them while leaving the code open source.

137 Recent events have shown that Internet shutdowns are becoming more and more frequent, in particular for political reasons.

138 S. Nakamoto (*op. cit.* note 124).

that follow Bitcoin's model are, for this reason, considered by purists to be the only "true" blockchains.[139]

III. Blockchain technology for the service of documents abroad

Blockchain technology is a major step in the evolution of information technology that cannot be ignored. Any plans to create a new system of international service of documents must take this recent technological development into account.

a) What improvements could blockchain make?

The Service Convention is part of a set of international conventions which are fundamentally aimed at ensuring access to justice across the world and facilitating the conduct of international civil proceedings. More specifically, this Convention aims to set up a system which ensures the service abroad of documents in a simple, efficient, and secure way that makes it easy to prove that the documents have been properly served. It is worth examining how blockchain technology could fulfil these fundamental objectives pursued in the context of the international service of documents.

Blockchain technology has the advantage of being extremely secure, and once information is put on a blockchain, it is time-stamped and tamper-proof. These two basic features of blockchain technology meet the essential conditions required for the transmission of documents for service abroad. Furthermore, the information stored on a blockchain could be easily accessible to authorities from anywhere in the world. Authorities could take immediate notice as the system would be accessible twenty-four hours a day, seven days a week. The use of blockchain technology would thus increase security, efficiency, and speed in the international system of service of documents set up by the Service Convention.

Considering the above, the use of blockchain technology for the transmission of all the documents that must be served abroad under the Service Convention could greatly benefit all Contracting Parties. If Contracting Parties were to jointly use blockchain technology in order to serve documents abroad, they would be operating on a widely accessible and secure network distributed across the world.

b) Permissioned or permissionless blockchain?

If the use of blockchain technology is considered in order to improve the operation of the Service Convention, the development of a permissioned blockchain would most likely be the first option examined. In this way, full control over the nodes of the network could be retained and the entire system could be maintained by the Permanent Bureau of the HCCH, a Contracting Party, or a central body to be determined. A permissioned blockchain is understandably the first type of blockchain that comes to mind when planning the development of such a system as part of the operation of an international convention.

However, while the need for control over the network by an authority seems evident in this context, the centralization of a permissioned blockchain poses security risks. This is

[139] Andreas Antonopoulos has defined the five pillars of a "real" blockchain, according to which a blockchain must be open, borderless, neutral, censorship resistant, and public. See A. M. Antonopoulos, The Five Pillars of Open Blockchains, 11 May 2019, available at: < https://www.youtube.com/watch?v=qlAhXo-d-64 > (last consulted on 16 March 2020).

due in particular to the limited number of nodes involved in the validation process of the blocks containing information and the centralization of their location. Unlike Bitcoin, which runs on an extremely large network of nodes that can be freely joined by users all across the world, a permissioned blockchain limits the number of nodes, which usually results in a small and centralized network. This centralization makes the network more prone to attacks, and information can be more easily corrupted as an attack would have to be launched on a limited number of nodes.

In addition, if all nodes are located in the same State, security risks are all the more increased. We could indeed imagine the possibility that access to the network, or to the Internet in general, could be restricted for any given reason in the State that hosts the nodes that validate the operations on the blockchain. A permissioned blockchain could also carry the risk of being censored by that government. In those two cases, there would be a risk that the entire system of international service of documents would be blocked.

By contrast, the use of a permissionless blockchain would significantly reduce security risks and would provide Contracting Parties with the full benefits of this new technology. The system would be fully decentralized, that is to say that data would be encrypted and then securely recorded in multiple places at the same time without a central data store and without any master copy. The multiplication of nodes, which could be located anywhere in the world, would provide the necessary degree of security to guarantee the availability and integrity of the information. All Contracting Parties could always have access to the information at any time, as a permissionless blockchain would not centralize control over the system in the hands of a particular State or a limited number of States. In addition, due to the distribution of data, the information stored could not be tampered. Those elements are essential when it comes to securely transmitting electronic data in a confidential manner at the global level.

Furthermore, by choosing to run the system on a permissionless blockchain, existing blockchains such as Bitcoin or Ethereum could be integrated in the data transmission process. This would significantly reduce development and operating costs as the most sensitive element of the system would be, so to speak, outsourced to an existing network which entails very little operating costs.

In our opinion, developing a permissioned blockchain would make as much sense as if a State were to create a private network similar to the Internet in order to share information at the international level.[140] Indeed, a permissioned blockchain would be a mere private network comparable to the Internet of the first age. The use of a permissionless blockchain as a new channel of transmission of documents in the context of the Service Convention would be the best way to provide Contracting Parties with a cost-efficient system that guarantees the integrity and availability of information.

However, we have to admit that relying on a permissionless blockchain for the data transmission process would result in a significant change in the operation of the Service Convention, as the system that would be used for the transmission of documents abroad would be partially outside the control of State authorities. The use of a decentralized technology means that States would no longer need to trust other States to establish a channel for communication and certification of information. But rather, States would trust blockchain technology to ensure the availability, authenticity, and integrity of the information issued and received. Furthermore, States would be bound by the available

[140] It should be noted, however, that some States are increasingly claiming the right to control and regulate the Internet. A permissionless blockchain would clearly run counter to this trend as it would not allow a top-down control of the system by governments.

technology offered by the chosen blockchain serving as the underlying network for the transmission of documents abroad. States would have no means to directly improve technical characteristics of the Bitcoin or Ethereum blockchain, such as scalability. This, however, would not mean a revolution in the way States operate. For example, State authorities commonly use the Internet as a means to transmit confidential information, even if they do not have full control over the network.

The use of a permissionless blockchain does not mean that the data transmitted in the context of the Service Convention would be accessible to all: encryption can guarantee the confidentiality of information. It is possible, for example, to use blockchain technology to create digital identity cards that are certified by a State with a digital seal. The system allows the information to be restricted so that only specific data is available. Similarly, access to information may be limited for each step of the transmission process of a document by determining what information is available and to whom. Confidentiality would therefore be ensured even if data was transmitted on a permissionless blockchain.

There are multiple possibilities to combine permissioned and permissionless blockchains, or even to combine blockchain technology with other systems, in order to take advantage of the characteristics of this new technology while obtaining various degrees of control over the system and distribution of data. Further research into blockchain technology could lead to finding a system that would provide the right levels of safety and control in order to meet the specific needs of Contracting Parties in the context of the Service Convention.

c) Does blockchain comply with the rules of law?

Relying on blockchain technology for the transmission of documents in accordance with the Service Convention would only be possible if the resulting system would conform at least to the principles of non-discrimination, technological neutrality, and functional equivalence. These three principles, which were first adopted in the UNCITRAL Model Law on Electronic Commerce, are considered fundamental when examining the compatibility of an electronic technology with the rules of law.

Under the principle of non-discrimination, the use of electronic means of communication shall not be discriminated against.[141] Therefore, the transmission of a document should not be denied legal effect, validity, or enforceability solely on the grounds that it took place on a blockchain. The use of blockchain technology does not preclude the transmission of a "written document" since the information is accessible so as to be usable for subsequent reference.[142] According to the principle of non-discrimination, the electronic transmission of the request for service, which consists of the model form and the documents to be served, must be considered as valid. Similarly, the requirement for an "original document" is met if there is a reliable assurance as to the integrity of the information from the time when it was first generated in its final form and if that information can be displayed to the person to whom it is to be presented.[143] Blockchain technology makes it possible to generate information that is time-stamped and tamper-proof, which clearly meets the requirements set out by the Service Convention as regards the formal requirements relating to the documents to be served. The use of blockchain technology

141 See *e.g.,* Art. 5 and Art. 11 of the UNCITRAL Model Law on Electronic Commerce; see also Art. 8 of the United Nations Convention on the Use of Electronic Communications in International Contracts (2005).

142 See *e.g.,* Art. 6 of the UNCITRAL Model Law on Electronic Commerce.

143 *Ibid.,* Art. 8.

can guarantee a higher level of security with greater efficiency and speed than the channels of transmission that are currently in use, in particular as regards the identification of the source and the content of the documents transmitted.

The Service Convention does not specify how the transmission of documents is to be performed, leaving room for the use of modern technology. From today's point of view, the Service Convention follows the principle of technological neutrality (even if this was not intended at the time of its adoption). The neutrality of the rules of the Service Convention makes it possible to take account of technological developments without the need for a revision of its text. The opportunities provided by the drafting of the Service Convention should be seized to make the most of modern technology. The use of new technologies should be considered in order to improve the operation of the Service Convention, in particular if the transmission process can be made faster.[144] A paperless transmission of documents would definitively foster the efficiency of international service of documents. The use of a technology such as blockchain, which permits instant transmission of documents from one State to another, would significantly improve the usefulness of the Service Convention.

The Special Commission proposed to examine each channel of transmission of documents provided for in the Service Convention by taking into account an approach based on the principle of functional equivalence as well as the objective pursued by the channel and its relevant requirements.[145] According to the principle of functional equivalence, the transmission of documents by electronic means may be regarded as equivalent to the transmission in paper form if it fulfils the same purposes and functions.[146] For example, the interpretation under the functional equivalence approach of the term "postal channels" found in Article 10(a) of the Service Convention allows us to consider that this channel of transmission could include fax, e-mail, SMS or the posting of a message on a website.[147] Likewise, the requirement of transmission of the judicial document or a copy in duplicate under Article 3(2) of the Service Convention must be interpreted according to the functional equivalence approach when the transmission is carried out by electronic means. Indeed, "[a]s a document transmitted by electronic means can usually be duplicated (copied and printed out) at any moment and an unlimited number of times, the requirement of a copy or duplicate will be satisfied by the sending of a single message".[148]

In accordance with the functional equivalence approach, the purposes and functions of the requirements set out in the Service Convention for the transmission of documents abroad should be examined in order to determine whether transmission via blockchain can fulfil those purposes and functions. For example, the "signature" of a document serves two essential functions: to identify the author and to confirm that the author agrees with the content of the document.[149] Blockchain technology respects these essential legal functions of a signature, as the use of a set of two cryptographic keys makes it possible to identify

144 See Practical Handbook (*op. cit.* note 114), Annex 8, No 11 f.

145 *Ibid.*, Annex 8, No 8.

146 See Art. 9(2) of the United Nations Convention on the Use of Electronic Communications in International Contracts: "Where the law requires that a communication or a contract should be in writing, or provides consequences for the absence of a writing, that requirement is met by an electronic communication if the information contained therein is accessible so as to be usable for subsequent reference."

147 However, Contracting Parties have divergent views on this topic. See Practical Handbook (*op. cit.* note 114), Annex 8, No 35-37.

148 *Ibid.*, Annex 8, No 18.

149 See *e.g.,* the UNCITRAL Model Law on Electronic Signatures (2001). See also Art. 7 of the UNCITRAL Model Law on Electronic Commerce, and Art. 9(3) of the United Nations Convention on the Use of Electronic Communications in International Contracts.

with certainty the sender of the message and to indicate that the sender approves the information contained in the message.[150] The Special Commission has already acknowledged that requests for service may be converted from paper into electronic form by scanning, or issued directly in electronic form, and signed in both cases by means of an electronic signature.[151] Those examples show that the principle of functional equivalence allows us to interpret the Service Convention in such a way that service of documents abroad can be achieved by using blockchain technology, without the need to revise the text of the Convention.

IV. Facing a new reality

Blockchain technology has all the characteristics necessary to simplify the service of documents abroad and improve the operation of the Service Convention. As of today, blockchain is probably the most suitable technology for transmitting documents abroad with efficiency, security, and speed. This technology has the potential to take the Service Convention out of an ancient world of papers and borders and propel it into the digital space.

The service abroad of documents using blockchain technology could probably be easily adopted in some States that already have a widespread use of computer technology. But it has already been observed that the transmission of documents by fax or by e-mail is not possible in all the Contracting Parties.[152] The fact that there is currently a discrepancy between Contracting Parties in the way in which they put into practice the channels of transmission provided for under the Service Convention does not seem to be a real obstacle to the adoption of blockchain technology. In countries facing difficulties in using electronic means for transmitting documents in accordance with the Service Convention, it is quite conceivable that the implementation of a new system for the operation of the Convention could be less complicated than in other countries that already use electronic means for the service of documents abroad. It may be easier to directly adopt a new technology than to deviate from a well-established practice. For example, in some countries, people have moved directly from a cash-based payment system to a smartphone payment system without ever switching to credit cards. Since a blockchain can be accessed with existing electronic devices connected to the Internet, such as a smartphone or a computer, the adoption of this technology for the service of documents abroad might turn out to be easier than one might think. This transition would be summarized in developing a user-friendly interface running on blockchain technology. This should be possible without too many practical difficulties, in particular if it can be carried out in a cost-efficient manner.

Contracting Parties that have a long-established practice for the transmission of documents under the Service Convention may be more reluctant to switching to a new channel of transmission. For example, in the field of legalization for foreign public documents, Switzerland is one of the first signatory States of the Apostille Convention that has been applied in this country since 1973. As of today, Swiss authorities do not use the electronic apostille register regardless of the obvious practical advantages it offers. In practice, a paper document on which the apostille is placed is indeed still required in most cases. However, Switzerland is not recalcitrant to the use of the Internet to facilitate communication between litigants and the authorities. Electronic communication with civil

150 See *e.g.,* Art. 6 of the UNCITRAL Model Law on Electronic Signatures: digital signatures based on cryptography enter into the scope of application of this model law.

151 See Practical Handbook (*op. cit.* note 114), Annex 8, No 13.

152 Conclusions and recommendations 2003 (*op. cit.* note 117), No 64; Conclusions and recommendations 2009 (*op. cit.* note 120), No 38.

courts has been allowed for many years, which enables service via electronic means.[153] However, even if e-mails are broadly used in Switzerland, litigants rarely use this means of communication and remain attached to paper when it comes to communicating with each other and with civil courts. These examples show that the implementation of a new system can be challenging, and it can only be achieved if users are willing to use it, especially when the system being changedworks.

The use of a new technology requires a change in mentality. The establishment of a global system of service of documents via blockchain could only work if all the parties to the Service Convention agree to give up on the use of paper and join this new electronic system. The greatest challenge would certainly not be the development and implementation of a new system, but its adoption by Contracting Parties. The revolution brought by blockchain technology is that the less the system can be controlled and the more distributed the data is, the more secure the network becomes. This new reality could initiate a paradigm shift in international civil proceedings if States were to recognize that security and integrity are not necessarily linked to centralization and control, but rather to decentralization of power and distribution of data. The transmission of documents to be served would no longer be hampered by State borders if documents could freely transit to their recipient on a distributed global network. This would significantly facilitate and secure international civil proceedings. However, such improvements can only be reached if both States and litigants switch to a new way of thinking.

153 See Art. 139(1) of the Swiss Civil Procedure Code (SR 272): "With the consent of the person concerned, summonses, rulings and decisions may be served electronically. They must bear an electronic signature […]."

HCCH a|Bridged
Edition 2019

brought to you in partnership with

Federal Ministry
of Justice and
Consumer Protection

ROPES & GRAY

Hague Conference on Private International Law
Permanent Bureau

Churchillplein 6b
2517 JW The Hague
The Netherlands

Tel.: +31 70 363 3303
Fax: +31 70 360 4867
secretariat@hcch.net
www.hcch.net

HCCH

Connecter Protéger Coopérer Depuis 1893
Connecting Protecting Cooperating Since 1893