LEGAL ASPECTS OF BLOCKCHAIN

JEROEN NAVES, BENEDETTA AUDIA, MARJOLEIN BUSSTRA, KOEN LUKAS HARTOG, YOSHIYUKI YAMAMOTO, OLIVIER RIKKEN, AND SANDRA VAN HEUKELOM-VERHAGE

A common denominator of Blockchain prototypes developed by governmental organizations is that they will prompt questions from administrative superiors. The primary question upper management will ask is, "With what laws and regulations must we comply if we want to open this service to the public?" More often than not, leaders of Blockchain pilots will not have a good answer to this question. This is because a large part of the legal community in the public sector has not yet dealt with legal questions surrounding Blockchain. However, a clear understanding of the legal implications involved will be required if Blockchain is to reach its full potential in the context of public administration and international organizations.

In the first half of 2018, the United Nations Office for Project Services and Blockchainpilots.nl, the Dutch government's pilot Blockchain program, brought together a group of legal and Blockchain experts from The Netherlands, Singapore, and the United States to produce a research volume offering an introduction to the legal aspects of Blockchain. This essay summarizes the findings from that book.

GENERAL REMARKS ON BLOCKCHAIN AND THE LAW

The decentralized nature of Blockchain makes it possible to view existing structures, which often are based on central databases, in a new light. This is evidenced by the rise of Bitcoin and other cryptocurrencies; in a relatively brief period, a financial system worth hundreds of millions of dollars was created without the involvement of any bank or government. It is a system that is difficult to grasp within our current legal frameworks, which is exactly why it is interesting from a legal perspective. There are regular calls for legislative changes and new regulations due to the existence of Blockchain technology. However, when looking at Blockchain on a transaction level, it is clear that many legal questions about Blockchain can be answered within current legal frameworks.

LAW IN A DECENTRALIZED WORLD

We are used to the idea that crossing a border changes a number of rules, from which side of the road we drive on to fundamental rights stemming from the United Nations Charter. The Internet has now blurred those national borders: with the press of a button on your computer, you can conduct a legal transaction within a country in which you are not physically located. Because our legal frameworks are based on national borders, it is highly relevant from a legal perspective which country any legal act has been performed in; this is relevant for which law applies and which government has the authority to enforce the law. However, the actual relevance of the law is limited; for instance, if I am in The Netherlands and I order a new pair of shoes from Italy via the Internet, all that really matters is that I get a good pair of shoes for a great price. Where the shoes come from is not legally relevant.

Blockchain technology takes the transborder attributes of the Internet from the level of information and communication to the level of transactions and contracts. The decentralized nature of Blockchain means that the system no longer needs to be linked to any legal system. The nodes that form a Blockchain can theoretically be located in any country in the world. However, a country also can declare that its laws apply to any nodes located within its borders. Should the other nodes in the network reject the applicability of these rules, the action of

ABOUT THE AUTHORS

Jeroen Naves works as an attorney at the Dutch law firm Pels Rijcken & Droogleever Fortuijn. Naves specializes in the legal aspects of disruptive technologies.

Benedetta Audia is the Corporate Legal Advisor and Head of the Commercial and Institutional law practice at UNOPS.

Marjolein Busstra works for the international law section of the Dutch Ministry of Foreign Affairs on human rights and cyber related issues.

Koen Lukas Hartog is the Programme Manager of Blockchain Projects for Dutch governmental organizations, Blockchainpilots.nl.

Yoshiyuki Yamamoto is the Special Advisor for UN Engagement and Blockchain Technology, UNOPS.

Olivier Rikken is Director Blockchain and Smart Contracts at AXVECO, where he works on sustainable Blockchain innovation implementations.

Sandra van Heukelom-Verhage is a lawyer at Pels Rijcken & Droogleever Fortuijn, the State Advocate of The Netherlands. She heads the Digital Transformation team.

The views expressed in this abstract may not necessarily reflect those of the United Nations and/or UNOPS.

the government in question means essentially nothing. In other words, the lack of a central database and a corresponding central party means that governments only have limited say about what does and does not happen in a Blockchain. It is interesting to see how a society deals with such legal and organizational issues. Take, for example, the Parity MultiSig Wallet.

Parity MultiSig Wallet

In July 2017, a "black hat" hacker—that is, a hacker with malicious intentions—discovered a flaw in the Parity MultiSig Wallet. Basically, the "names" of the signatories (the externally owned account numbers) could be overwritten without any checks, meaning that the hacker was able to overwrite him-/herself as signatory multiple times. This enabled the hacker to sign the minimum required *M* times by him-/herself and transfer funds without authorization. This hack began on July 17, 2017.

The first victim of the hack was an Ethereum startup that actually had ties to some "white hat" hackers—ethical hackers who look for flaws in systems and warn others about any vulnerabilities they find. The Ethereum startup immediately warned the white hat hackers about the suspicious activities. This resulted in a race between the white hat hackers and the black hat hacker(s).

An important element of Blockchain is its transparency, which played a crucial role in the counter-actions to the black hats. Just as it is possible to see all transactions in permissionless Blockchains, it is also possible to search for smart contract code, which means that the addresses of other Parity MultiSig Wallets were easily found. This is what the white hat hackers did, and, using the flaw found by the black hat hacker, they transferred the funds from the vulnerable wallets into safe accounts. They then posted on various online platforms that, if the rightful owners were missing their funds, they would need to prove that the wallets belonged to them, after which the funds would be transferred to new, secure accounts. The race ended with the black hat hackers getting away with approximately $35 million, while the white hat hackers recovered almost $360 million. This is a good example of unexpected governance actions resulting from the characteristics of Blockchain and the cooperation of the Blockchain community.

THE USE OF BLOCKCHAIN TECHNOLOGY IN CURRENT LEGAL PRACTICE

Blockchain offers a different way of looking at the current legal system. This does not mean that Blockchain technology does not raise important questions within current legal frameworks; a number of such questions are answered below. It is possible that certain industry-specific regulations will apply to Blockchain; for instance, a Blockchain in which electricity is traded must meet the applicable regulations within the energy industry.

Applicable Law

The decentralized nature of Blockchain technology means it is not possible to determine which laws apply generally to Blockchain, because every legal area sets the conditions for applicability within its domain. Thus, it is conceivable that Dutch civil law will apply to a Blockchain transaction while the German authorities can levy taxes on the same transaction. In fact, regulations from many different legal systems could apply to a Blockchain, depending on the context.

At the transaction level, it is usually quite clear which laws apply. If a Blockchain transaction is executed between two parties in the same country, then the civil law of the country in question generally will apply.[1.] However, inter-

national private law will have to determine which civil law applies to a transaction between parties from different countries. For example, if a transaction takes place between parties from two different European Union countries, the Rome II Regulation creates a harmonized set of rules to govern the choice of law in civil and commercial matters (subject to certain exclusions) concerning non-contractual obligations. The general rule is that parties can decide in advance among themselves which laws apply to their Blockchain transaction. If they do not do so, then the laws of the country where the characteristic performance is executed will generally apply.

Identity in a Blockchain

All transactions on open (non-permissioned) Blockchains are public. This does not mean it is always clear who has executed the transactions in a public Blockchain. In the Bitcoin Blockchain, for example, all users have a public key and there is no way to determine who is behind a key. It also is not possible to determine who is behind a specific account through a central organization because no central organization regulates the Bitcoin Blockchain.[2.]

In practice, this could lead to problems. If you do not know who you are transacting with on a Blockchain, it is practically impossible to take that party to court if something goes wrong with the transaction. It is conceivable, for instance, that you make a payment with Bitcoin and accidentally enter an additional zero, which means ten times as many Bitcoins as intended are transferred to the receiving party. If such a transaction had taken place through a bank, it would be relatively simple to find out the identity of the receiving party and force repayment judicially. For a Blockchain transaction, finding out the identity of the receiving party is simply much more complicated.

Several initiatives are under way to develop a way to link the biological identity of a person to a digital identity by means of a Blockchain or otherwise.

Human Rights and Blockchain

From a human rights perspective, Blockchain is both a gift and a threat. The right not to be discriminated against, to privacy, and to remedy are especially at risk. To make sure the positive impact greatly outweighs the negative, human rights must be taken into consideration from an early stage in the development and implementation of Blockchain applications, as well as in broader discussions about the governance of Blockchain and related technologies. Human rights by design is a crucial principle, as many of the human rights issues identified in this article can only be tackled in the beginning phase of a new application. The right to privacy is especially vulnerable in this context because of the special Blockchain characteristic that data, once submitted, cannot be changed or deleted. This means that mistakes made with regard to personal data cannot be undone. Moreover, whereas the right to privacy requires consumers' informed consent for the use of personal data, there is a risk that Blockchain applications are so technically complex that they will defy the average person's understanding.

Even though businesses and other private actors have the responsibility to respect human rights, they tend to need encouragement from the government, especially where human rights-friendly solutions cost money. This means that states should actively follow developments, participate in debates, and act in a timely manner to get their regulatory bodies in order. They must make choices that promote and reinforce human rights before the technical reality makes those choices for them.

A considerable number of the points made in this article are not exclusively relevant to human rights but stem, rather, from a more general unease between the current legal paradigm, which has a human focus, and the digital paradigm, which is binary in nature and applies a logical, mathematical focus. This tension will only increase as Blockchain technology enters the phase of autonomously creating smart contracts and autonomous organizations. Not all technologies are the same, however. For instance, there is a fundamental difference between permissioned Blockchains and unregulated, permissionless Blockchains. As permissioned or regulated permissionless Blockchains run by certain rules, they can be regulated more easily and forced to fit into current legal systems. Unregulated permissionless Blockchains, however, pose some fundamental challenges in terms of governability and accountability that cannot easily be solved. They call for multidisciplinary, multistakeholder debate about how to make sure they live up to their revolutionary potential in a way that is consistent with human rights and the rule of law. Technological experts and lawyers have so far operated more or less independently; the challenges outlined in this article make it clear that this cannot continue. Legal and technical experts need to team up to devise solutions that are technically feasible and respectful of human rights.

Blockchain and the UN

Use of Blockchain protocols in development is as new as it is promising. The UN system is in a unique position to apply these protocols, due to the reach of its operations, its independence, and its institutional experience. Because organizations in the UN system have enough regulatory flexibility to work with and refine Blockchain platforms under current circumstances, UN activities might serve as a kind of test lab both for Blockchain systems and for new regulatory approaches to Blockchain-based international transactions. As noted at several points in this chapter, a solution to the lack of direct hierarchical representation within complex Blockchain systems could be the creation of third-party entities to serve as contractual intermediaries between decentralized autonomous organization-type communities and regulatory mechanisms or third-party partners.

Some have suggested that the United Nations Commission on International Trade Law (UNCITRAL) play a central role in outlining a regulatory framework for this process.[3] Within existing UNCITRAL works, including the Model Law on Electronic Commerce, the Model Law on Electronic Signatures, the Convention on the Use of Electronic Communications in International Contracts, the Model Law on Electronic Transferable Records, and others, it appears that these existing structures can account for the use of Blockchain exchange systems with some flexibility. However, enough exceptions exist to provide incentive for UNCITRAL to develop new works to account directly for cryptocurrencies and other Blockchain-enabled transactions. For example, Koji Takahashi notes that the ST Model Law defines the word "money" as legal tender authorized by a state.[4] Bitcoin and other cryptocurrencies could meet this definition if a state legally adopted it as valid currency but, looking further, a cryptocurrency cannot qualify as a "tangible asset" under ST Model Law Article 2(ll) and therefore cannot be treated directly as money under this regulatory model.[5] It is therefore recommended that UNCITRAL develop new works specifically to provide an international model for the regulation of cryptocurrencies. While current frameworks regulating international financial transactions do not tend to disallow the use of cryptocur-

rencies per se, if such mechanisms are to become a stable and widespread source of development funding, it is inevitable that more fine-tuned regulatory structures will arise to deal with the inevitable conflicts that arise.

UNCITRAL, with its resources and history of legitimacy in this area, is ideally situated to step into this niche.[6.] Given that the UN public mandate puts UN system organizations in a position to be early developers for a range of Blockchain protocol types, it is especially appropriate, and reflective of its international accountability, that the UN system take on a corresponding normative role.

---

1. Deviation from this is only possible if the parties have agreed by contract that a different law applies.

2. The legal entity behind a public key is generally known to the party that exchanges Bitcoins or other cryptocurrency into euros or dollars. Investigative services, for example, could find out who is behind a transaction in the Bitcoin Blockchain through this exchange office.

3. de Caria, Riccardo. *A Digital Revolution in International Trade? The International Legal Framework for Blockchain Technologies, Virtual Currencies and Smart Contracts: Challenges and Opportunities.* UNCITRAL, 2017.

4. Takahashi, Koji. *Implications of the Blockchain Technology for the UNCITRAL Works.* Available at https://onedrive.live.com/?authkey=%21AMLDDJc03VocQms&cid=431D6C57123F90CF&id=431D6C57123F90CF%212163&parId=root&o=OneUp, p. 9.

5. Takahashi, *Implications of the Blockchain,* p. 10.

6. Takahashi, *Implications of the Blockchain,* p. 9.