Blockchain and the law. An exploration of the need for regulation.

Maurice Schellekens, Eric Tjong Tjin Tai, Wesley Kaufmann, Femke Schemkes and Ronald Leenes

Tilburg University, June 2019

Summary

Introduction

Blockchain is a technique from which much is expected and to which many qualities are attributed. Blockchain makes it possible that parties who do not know each other and probably do not trust each other can trade safely with each other. Many traditional intermediaries, so-called trusted third parties would become superfluous. Blockchain thus leads to efficiency gains and cost savings because many functions can be automated. Blockchain would enable new forms of collaboration and blockchain is of value to the internet.

It is a technique that, based on the above expectations, can considerably change existing relationships within society. Values and interests can come under pressure. This raises the question of the acceptability of blockchain in the different forms it can take. This report establishes a framework with which the opportunities and risks associated with the technology can be weighed and that the legislator offers a first tool to assess the suitability of the current legal framework.

Blockchain technology

A blockchain is essentially a database of which many copies are kept under different managers. A distinction is made between so-called permissionless and permissioned blockchains. Everyone can freely join a permissionless blockchain as a manager. Coordination within the blockchain, for example for the execution of a payment with cryptocurrency, is in principle not based on agreements or contracts made in advance, but on a system of crypto-economic incentives. In a permissioned blockchain, only authorized managers can be active. There may be a central body that controls access or this may be left to the incumbent managers together. Coordination within a permissioned blockchain can be based on a system of crypto-economic incentives, but that is not necessary. It can also be based on mutual agreements.

In this report, four properties are attributed to block chains: they are immutable, a blockchain is in principle blind, a blockchain is redundant and a blockchain is technically transparent.

The immutability essentially only applies to blockchains based on a system of crypto-economic incentives. The immutability essentially means that an individual manager cannot change what is seen as the content of the blockchain. If an individual manager changes old data in his copy of the blockchain, his copy would no longer be seen as a valid copy of the blockchain. The manager disqualifies himself as it were. If a number of managers work together, the content of the blockchain can be changed, but this is not easy and therefore of little practical importance. A blockchain based on agreements can provide for the possibility of changing old data.

Blindness of the blockchain essentially means that there is no guarantee that data included in a blockchain is correct. When recording new data, it can be checked whether the new data is consistent with old data in the blockchain, but this is only a limited check. New data to be recorded

can possibly be checked on the basis of data outside the blockchain (entered via a so-called oracle), but it is unclear how reliable that data is. In short, data is not correct just because they are included in a blockchain.

Redundancy indicates that there are multiple copies of a blockchain. Redundancy can offer benefits in terms of safety, but it can also be a burden. Everything that is realized within a blockchain requires coordination. If the blockchain is not based on agreements, dependence will arise on what the technology does and does not coordinate.

A blockchain is transparent in a technical sense. In order to determine which copy or version of a blockchain is valid, it must be possible to inspect blockchains in their entirety. For many applications, however, it is not convenient that all data must in principle be available for inspection.

A smart contract is code that is placed on a blockchain and executed by managers of the blockchain. A smart contract does not have to provide a legal agreement. In principle, it is just code. Once it has been placed on a blockchain, the code can no longer be changed, not even by the person who placed the code on the blockchain.

General legal aspects

The research underlying this report has analyzed a number of general legal aspects.

Parties that want to conclude an agreement on the blockchain can use a smart contract for this. The claimed advantage of a smart contract is that it would record and implement the entire agreement between the parties. Execution of the agreement is therefore automatic and guaranteed. That would remove an important source of conflicts about agreements, so that it would not be necessary and even undesirable to seek judicial intervention.

A smart contract is not itself an agreement but can be considered as proof of the conclusion of a legal agreement. The content of that agreement is determined according to legal rules. The program code of the smart contract will be important to determine the content of the agreement, but it is not decisive. The intention of the parties also plays a role. It can be difficult to lay down all the usual rules of an agreement in a smart contract in an understandable way. If the rules of a smart contract conflict with what follows from the legal agreement, a party can in principle ask the court to correct the implementation of the smart contract. It is possible that such attempt at legal enforcement is not effective.

Smart contracts have various disadvantages and risks. Smart contracts usually require payment in advance, which leads to interest loss and currency risks. They can only implement the normal rules of contract law to a limited extent: that may mean that protection that a party has in law (such as in the case of force majeure) cannot be obtained. When using human "oracles" for the assessment of circumstances, the smart contract becomes dependent on human intervention again and does not execute automatically. Smart contracts cannot be understood or controlled without specialist knowledge, and hiring such knowledge is costly, while it is risky to trust that the contract does what the developer says it does. Smart contracts also deviate substantially from the normal way in which people view a contract: as a part of an interpersonal relationship, which does not regulate in detail how to deal with different circumstances.

Smart contracts can offer benefits in certain circumstances despite the risks. This seems to be the case in particular with agreements with anonymous parties abroad, or as part of a larger ordinary agreement (where the smart contract is used as a part of that agreement).

Another important general topic is the General Data Protection Regulation. The controller plays an important role in guaranteeing adequate processing of personal data under the GDPR. Due to the P2P character of blockchains, it can be difficult to determine who the controller(s) is (or are), especially if applications are included in the core code (such as native crypto currencies). Even if a controller can be designated, it is difficult for this person to adequately shape the responsibility. To achieve something within a blockchain (such as deleting data), coordination between managers is required. The coordination needed to meet the rights of data subjects is not supported by the technology and sometimes even counteracts compliance with the GDPR. It is the difficult task of the controller(s) to achieve this coordination in any way.

Another tricky issue under the GDPR is the erasure of personal data in the context of data minimization and the right to be forgotten, for example. In blockchains based on a system of crypto-economic incentives, this is not possible in practical terms. It is currently unclear whether this tension will be resolved by opting for a different type of blockchain or putting into perspective what 'erasure' means under the GDPR.

Use-cases

Four use-cases were investigated for the purpose of this report.

The ship registration

The use of a permissionless public blockchain for the ship register leads to a shift in costs and time (from initial registration to later transactions) and results in a lower reliability of Dutch ship registration. In addition, there are risks of fraud, privacy, and abuse for money laundering, etc. For the Netherlands, because of the high-quality ship registration that exists here, a permissionless public blockchain is therefore not a useful option. Other blockchain variants are possible but do not have the benefits of a permissionless public blockchain. Depending on the chosen structure, legal rules will also have to be adjusted to a greater or lesser extent.

Treasury banking for the benefit of the new construction of schools

In this use-case, particular attention was paid to the usefulness of blockchain as a means of accountability. One of the tasks of the Auditdienst Rijk (national audit service) is to check whether the financial management of the Central Government meets standards of efficiency, legality, orderliness and verifiability. A blockchain that structures treasury banking for the construction of a new school building will probably simplify controls by the Auditdienst Rijk. However, two comments can be made. In the first place, simplified control can also be realized without a blockchain. Secondly, a blockchain implementation does not cover all dimensions that the Auditdienst Rijk wants to control. A blockchain does not make the Auditdienst Rijk superfluous.

The transport of waste within the EU

The European Regulation on shipments of waste does not stand in the way of the digital execution of the relevant processes. In this respect, implementation in a blockchain would be possible. However, the impossibility of deleting personal data placed on the blockchain is a point of concern. In addition, physical checks remain necessary. Shipments that have never been entered in the blockchain the blockchain does not know about. If data entered does not correspond to reality, the blockchain itself cannot determine this. It is not clear what the benefit of a blockchain implementation is compared to a traditional automation process.

The sharing of privacy-sensitive data by the government - the CAK

These use-case concerns complicated invoicing processes within the framework of the Social Support Act. In this use-case, automation of work processes can mean significant progress. The benefit of blockchain is not clear. A blockchain implementation has important disadvantages in the field of data protection: data cannot be erased and it is difficult to correct data. To guarantee the confidentiality of personal data, data is stored off-chain. The question is whether this will remove the potential benefits of using a blockchain.

Synthesis

Legal framework

Charting the various legal aspects of blockchains requires a structure that can function as an ordering principle. To this end, criteria for acceptability of normative technology have been chosen. Blockchain is normative technology. Its purpose is to redefine the relationships between the parties involved. Moreover, the chosen scheme of criteria is sufficiently general to give a broad picture of legal aspects. Here the four most important criteria are discussed.

Human rights and moral values / protection function of law

Which human rights and moral values come under pressure with blockchain? Some come under pressure quite explicitly, in other cases it is more an implicit process. The most important ones that emerged in this study are the ones listed below.

The human rights that explicitly come under pressure include privacy and data protection, as already shown above.

Autonomy is under pressure. Information obligations towards users are unclear and blockchain applications leave little room for accommodating the autonomy of the user. The automated execution of processes based on a limited set of data (blindness of the blockchain) entails a risk of unequal treatment and discrimination.

Blockchain can also implicitly lead to the undermining of legal standards. The blockchain / smart contracts channel behavior and the applicable legal standard disappears from view. The code will take over the role of the law in the minds of those involved. Here is reason to keep your finger on the pulse.

Legitimacy

It is often claimed that a blockchain would make trust superfluous. However, it is often overlooked that the code for the blockchain or for the smart contract contains many choices. Instead of believing that trust has become superfluous, it is better to ask yourself what the legitimacy of exercising power through code is. The legitimacy has a formal aspect (administrative action requires a legal basis, private parties are, in principle, free to act), but also a guarantee aspect: sufficient safeguards must be built in to prevent the simple user from surrendering to the arbitrariness of the builder of the technology. Care should be taken to ensure that block chains do not compromise guarantees and legitimacy in the name of promoting innovation or efficiency. Democracy and transparency of rules

Blockchains have implications for many people who have not been involved in the development of the code that those implications bring about. This raises the question of the democratic legitimacy of blockchain: to what extent are those affected by blockchain involved in shaping a blockchain or blockchain application? The most important permissionless block chains have a governance structure in which everyone can participate, but the decision-making power nevertheless lies with miners and core code developers. Especially, if the social impact of block chains increases, effective governance is an important point of attention.

Proportionality

Blockchain is used for a variety of purposes. Achieving efficiency gains (better services, lower costs) is, according to the use-cases, a dominant motive. At the same time, human rights and moral values can come under pressure with blockchains. Is a blockchain a reasonable means of achieving the goal (efficiency gain)?

In the first place, the claim that a blockchain leads to efficiency gains must be mitigated. A blockchain does not solve the problem of the authenticity of data entering the blockchain. Guaranteeing authenticity requires communication with the "outside world" (for example traditional intermediaries) and efficiency is lost there. Just looking at the work of the nodes is too narrow a perspective and does not give a complete picture of the (in) efficiency.

The claim that blockchain solves problems with fragmented work processes, such as with the ship register, is debatable. All required data may be available on the blockchain for every relevant party, but this has not yield a workflow. Integration and assessment of the data in a work process requires a separate layer in software that will have to be placed on top of the blockchain. As this does not (yet) exist, the question arises again whether a traditional IT implementation of the work process is or cannot be more efficient.

In particular, blockchains that function on the basis of crypto-economic incentives have important disadvantages: problems with the unchangeability of data, doubts about scalability and blockchains who work with proof-of-work, sustainability concerns.

In conclusion, it can be said that this report is critical of blockchains. That does not mean that where blockchain offers opportunities they not be seized. Blockchain, however, does not appear to be the cure for all ailments, and permissionless blockchains in particular have side effects. When considering new blockchain projects, it is important to first make a good problem analysis and carefully examine whether a blockchain offers a solution for the identified problems. If this is the case, the framework elaborated in Chapter 5 provides a first tool for mapping out legal preconditions and thus turning it into a socially responsible innovation.