In: Blockchain Technology and Applications II ISBN: 978-1-53617-931-6
Editor: Jan Veuger

Chapter 5

LEGAL ANALYSIS OF BLOCKCHAIN APPLICATIONS

Lesley C. P. Broos[1], PhD and Nelleke Jans[2]
[1] Lawyer in the areas of intellectual property law, IT law and privacy at KienhuisHoving advocaten en notarissen, Assistant Professor of Business law and technology at University of Twente, the Netherlands
[2] Corporate lawyer at KienhuisHoving advocaten en notarissen

ABSTRACT

In this legal analysis, the authors examine a number of legal complications involved with the use of blockchain technology. These include aspects relating to the law of obligations, the law of property, intellectual property and privacy as well financial supervision (and developments in it). Based on real-life examples of a permissioned blockchain application (Mijn Zorg Log [My Healthcare Log]) and a permissionless blockchain application (Bitcoin), the authors on the one hand show how existing laws and regulations can be applied to this new phenomenon and, on the other hand, they state what amendments to laws and regulations are indicated in order to eliminate legal uncertainty, a factor that can stand in the way of such blockchain-driven innovations.

Keywords: blockchain, privacy law, the Dutch Money Laundering and Terrorist Financing (Prevention) Act (*Wet ter voorkoming van witwassen en financieren van terrorisme* ("Wwft")), General Data Protection Regulation ("GDPR") (*Algemene Verordening Gegevensbescherming*), intellectual property, private international law, smart contracts, initial coin offerings, financial supervision, cryptocurrencies, permissioned blockchain, permissionless blockchain, Bitcoin, Ethereum, tokens, Mijn Zorg Log

1. INTRODUCTION

Blockchain is hot. Experts consider the advent of blockchain to be the biggest digital development since the invention of the internet. This is because blockchain technology is regarded as safe, efficient and reliable and therefore potentially suited to the design and reorganisation of various processes within and between organisations. It is these and other properties that have propelled its lightning development in recent years.

We currently see applications of this technology in both the public and private sectors. The Dutch Ministry of Internal Affairs (*Ministerie van Binnenlandse Zaken*), for instance, sees potential in blockchain technology, for both government and society, for protecting fundamental rights and public values.[1] For this reason the Dutch government has, in recent years, been exploring whether and to what extent blockchain technology can be applied to existing processes. It has set up pilot projects to identify the opportunities the technology offers, built prototypes and implemented a number of initial projects.

The private sector is also examining blockchain technology and the possibilities it opens up. According to the software developer Topicus, it is

[1] https://www.digitaleoverheid.nl, section "*nieuwe technologieën, data en ethiek*" (consulted on 2 March 2020) [in Dutch].

expected that almost half of Dutch businesses will be investing in blockchain technology in 2020.[2] Nearly one in five companies is already using blockchain in their existing processes.

The growing number of blockchain applications is also raising legal questions. Some of these can be answered on the basis of existing (usually 'technology-independent') laws and regulations and the 'open standards' that they often encompass. It is therefore logical for legal experts to legally classify – where possible – events in and around blockchain technology. Accordingly, the mere fact that there are legal question marks about a relatively new technology does not mean that legislation needs to be amended right away. The law of obligations, for instance, still seems flexible enough to accommodate the use of blockchain and to classify actions in the blockchain in legal terms.

However, some legal questions about the application of blockchain technology cannot be answered with certainty on the basis of current laws and regulations because they require too much interpretation of the rules (which were not written for blockchain applications), therefore creating the risk of legal uncertainty, or because a suitable legislative framework is simply lacking. Here lies a possible role for lawmakers and, where this is the case, we will point it out.

The Dutch courts have also issued findings on a number of issues in this regard. In 2014, for instance, the Overijssel District Court (*Rechtbank Overijssel*) had to legally classify the cryptocurrency Bitcoin for the first time.[3] It determined that Bitcoin is not 'money' but rather a 'means of exchange'. In 2018, the Amsterdam District Court had to determine whether a claim in cryptocurrencies is a claim that can be submitted as a second creditor's claim in insolvency proceedings. It answered the question in the affirmative. A bitcoin has characteristics of a proprietary right (*vermogensrecht*) and can therefore be regarded as a second creditor's claim (*steunvordering*).[4] Incidentally, both of these judgments were issued by

[2] This was the conclusion of the Future of IT survey of 400 IT decision-makers and co-decision-makers commissioned by Topicus.

[3] Overijssel District Court 14 May 2014, ECLI:NL:RBOVE:2014:2667; Prg. 2014/177; RCR 2014/64.

[4] Amsterdam District Court 14 February 2018, ECLI:NL:RBAMS:2018:869.

'lower courts' and they have not yet been upheld by the Dutch Supreme Court (*Hoge Raad*).

This legal analysis provides a layperson's guide to a number of legal implications of the use blockchain technology based on currently applicable Dutch laws and regulations and interpretations of them. We will examine a number of more generic areas of law which play a role in most blockchain applications. We note in this regard that blockchain applications may also be subject to sector-specific rules. However, a profound analysis of each area of law that might potentially be relevant is beyond the scope of this publication.

Section 2 looks at the more generic areas of law that could be relevant to the application of blockchain technology. Section 3 then examines two real-life examples and applies the areas of law mentioned in section 2 to them. We will note the existence of any sector-specific rules but will not examine them in detail. Section 4 concludes with a number of closing observations.

2. Application-Independent Areas of Law

Blockchain applications touch on various areas of law. This means that there are no 'blockchain' lawyers. Legal scholars from various legal disciplines will need to look at blockchain technology, its applications and their legal implications.

The use of blockchain technology raises questions involving both public and private law. Public law deals with the rules that apply between government and private parties. The 'principles of sound administration' (*algemene beginselen van behoorlijk bestuur*) are an important aspect of public law. When using blockchain applications in the fulfilment of their public duties, public authorities are (as always) required to observe these principles which include the duty of due care and the principle that reasons must be given.

Private law deals with the rules that apply between private parties. These rules are spread over various legal areas (such as property law

(*goederenrecht*), the law of liability (*aansprakelijkheidsrecht*) and the law of obligations (*verbintenissenrecht)*), they are enshrined in the Dutch Civil Code (*Burgerlijk Wetboek*) and they answer questions such as: how is property transferred legally? Who can be held liable for damage caused by another party? Is there a legally valid contract between contracting parties?

This analysis focuses on private law because the particular aspects of public law are only relevant to specific blockchain applications in which a public authority acts for example as a user when fulfilling its public duties. Private law questions which arise in the use of blockchain technology must be answered by classifying acts in a blockchain on the basis of the system and terminology of the Dutch Civil Code.

2.1. Contracts

A basic premise in the Dutch law of obligations is that there is no prescribed form for concluding a contract. This means that, subject to the exceptions provided by law,[5] a contract can be concluded verbally, in writing or in digital form. Accordingly, concluding a contract on a blockchain can have just as much legal effect as concluding one outside it.

For there to be a contract, there must be an offer and the acceptance of it (*aanbod en aanvaarding daarvan*),[6] i.e., a party who offers something and another party who accepts it, along with the conditions attached to it. If significant aspects of such conditions are not accepted, or are only accepted in part, then there is no valid contract. Without the acceptance of an offer, no contract is concluded. There is only one exception to the principle of 'offer and acceptance' being sufficient, where the law prescribes additional requirements for the conclusion of a certain type of contract.

Another issue involved in the law of obligations is the relationship between the parties on a blockchain. The parties who enable transactions on

[5] Certain contracts require, however, a particular form. Under the Dutch Copyright Act (*Auteurswet*), for example, copyright transfers are only legally valid if they are based on a written document (*akte*); in addition, according to the General Data Protection Regulation, a processing contract between a controller and a processor must be in written or electronic form.

[6] Article 6:217 of the Dutch Civil Code.

a blockchain are also known as nodes. How should the relationship between them be classified? Do they actually have a legal relationship?[7] Is there a contract between the nodes who act on the blockchain and the operator of the platform in question? These questions cannot be answered without analysing the actual application, as all the events and acts on the blockchain need to be assessed on the basis of the Dutch law of obligations. Answering these questions requires a distinction between 'permissionless' and 'permissioned' blockchains.

Joining a permissionless blockchain is not subject to any special conditions. Permission from the node manager or operator of the blockchain platform is not needed in order to join the blockchain and to carry out acts on it. Consequently, merely joining a permissionless blockchain does not give rise to any reciprocal rights and obligations,[8] nor to a contract, although it does give the appearance of *de facto* cooperation. This does not, of course, alter the fact that the parties could still conclude a contract among themselves, with rights and obligations (possibly implementing it in a 'smart contract'). Another possibility is that there is a pre-contract that already regulates the legal relationship between the parties involved. Joining the blockchain could be part of such an 'off-chain' pre-contract. A pre-contract can serve as a framework for arrangements between the parties and thus create clarity. We will illustrate this using an example based on the Decentralized Autonomous Organization (DAO) application.

The DAO consists of a number of linked smart contracts and is thus an autonomous organisation in which transactions can be performed on the basis of code.[9] DAO was launched by the Ethereum platform for making investment proposals. Every Ethereum user could join a proposal by transferring a particular amount. The proposal had the form of a smart contract. Because there was a flaw in the code of a particular smart contract, hackers succeeded in emptying the investors' accounts. A change to the code

---

[7] A legal relationship is the legal relationship between parties, for example based on the law or a contract.

[8] Apart from possible (copyright-related) rights and obligations arising from a licensing contract (usually an open source license) if and to the extent it applies to the relevant blockchain application.

[9] Veuger, J. (2020), Blockchain Convergentie, p. 43 [in Dutch].

was then proposed, i.e., an update, to prevent a similar situation from occurring again. However, the nodes did not have to accept the update. Accordingly, some of the nodes accepted it while others did not. This led to the existence of several versions of the code (known as 'forking'),[10] which was of course an undesirable situation. The nodes could instead have concluded a pre-contract obliging them to accept updates and thereby to prevent forking.

Not every blockchain application is suitable for widespread public use. In certain instances or sectors, such as healthcare, there is a desire to regulate access to particular blockchains. This was the reason for creating permissioned blockchains, which require the manager's permission to join them. Joining can be regulated in various ways. In all cases, anyone wishing to join a blockchain has the right to do so, but the other parties to it expect something in return. Acceptance of a new member therefore gives rise to reciprocal rights and obligations, and joining and admission can be classified as an act with legal meaning. A legal relationship therefore comes about.[11]

To sum up: joining a permissionless blockchain, even though it can be legally classified as *de facto* cooperation, does not lead to the existence of reciprocal rights and obligations. On the other hand, joining a permissioned blockchain can create a legal relationship between the parties to it and, accordingly, give rise to reciprocal rights and obligations.[12]

Another relevant question involving the law of obligations is how smart contracts should be classified. Smart contracts can be used to do a lot of interesting things. They can be used for tokenization, to code and automate business processes and to hard code agreements between parties involving value and other types of asset transfer (such as escrow agreements). A smart contract is a program that can be run on a blockchain based on the principle "if this, then that." This means that the 'contract' performs itself when a

[10] Forking of Ethereum into Ethereum and Ethereum Classic.

[11] Smart Contracts Werkgroep ('Smart Contracts Working Group') - Dutch Blockchain Coalition. Smart Contracts as a specific application of blockchain technology. Initial exploration of questions about laws and regulations and training requirements as a result of blockchain and, more specifically, smart contracts.

[12] Schellekes, M., Tjong Tjin Tai, E., Kaufmann, W., Schemkes, F. and Leenes, R (2019), Tilburg University, Blockchain en het recht. Een verkenning van de reguleringsbehoefte [in Dutch].

certain pre-programmed event occurs.[13] In that case the performance of a smart contract is strictly deterministic, in line with the rules designed by its creator.[14] Smart contracts can be effective in situations where parties trust each other enough to agree on the consequences of encoding their agreement in a smart contract and – by doing so – automating the implementation of their contract.

A smart contract is in fact code. Can a smart contract be regarded as a contract in the legal sense? We have already seen that acceptance of an offer is needed for a contract to be concluded. According to the literature, a smart contract can have legal meaning, but that is not necessarily the case.[15] The fact is that, in principle, a smart contract is not a contract in the customary (legal) sense.[16] It *can* create obligations, but that will always depend on the content of the code and all other relevant circumstances, like the intentions of the contracting parties.

Accordingly, whether obligations are created by smart contracts (and their performance) depends on several circumstances, including how the smart contracts manifest themselves. For instance, a smart contract might contain suspensive conditions or conditions precedent, or it might automatically perform a particular process. These acts are acts of implementation. But a smart contract might also bring about a contract or a decision governed by public law.

The offer and acceptance mechanism requires parties to be aware of the substance of the offer. Consequently, in the case of a smart contract, programming expertise would be necessary and the programmer's commentary on the source code would have to be provided, or the contents of the offer would have to be set out in writing in a (traditional) contract. These options are not always applied in practice. For instance, the smart contracts in the Ethereum Blockchain – the most frequently used blockchain

---

[13] Schuringa, H., *Enkele civielrechtelijke aspecten van blockchain, Tijdschrift voor Computerrecht* 2017/254, afl. 6, p. 249-291 [in Dutch].

[14] Szabo, N. (1997), *The Idea of Smart Contracts*, at http://szabo.best.vwh.net/smart_contracts_idea.html (consulted on 2 March 2020).

[15] Tjong Tjin Tai, E., NJB 2017/146, p. 179-182 [in Dutch].

[16] De Vries, E. (2019), *Smart Contracts: een keten van vertrouwen reikend tot in de fysieke wereld* [in Dutch].

for smart contracts – are all placed on the blockchain in bytecode form.[17] For users of Ethereum without knowledge and expertise about programming it will be difficult to inspect such code.

2.2. Property/Intellectual Property

Dutch property law deals with real rights (*zakelijke rechten*) (e.g., the ownership of objects) and proprietary rights (*vermogensrechten*) (meaning for example a monetary claim). The use of blockchain technology frequently raises the question of who actually owns the blockchain. A question that might precede this is whether anyone 'owns' it at all. According to the Dutch Civil Code, ownership is the most comprehensive right that a person can have to an object. Accordingly, a person can only own objects. Objects (*zaken*) are tangible things subject to human control.[18] An object therefore has to be tangible. A blockchain is in fact a distributed database in which information is stored. This means that a blockchain cannot be considered to be tangible and that – on the basis of Dutch law – no one can own one as such. A person can, however, have intellectual property rights to a blockchain (or parts of it). The underlying software might for instance be copyright protected (provided that it has an original character and bears the personal imprint of the maker).[19] In addition, it is possible for there to be database rights to a blockchain's content (provided that the compiler(s) of the data stored in the blockchain has/have, for example, invested substantially in the collection and organisation of the elements stored in the distributed database).[20]

Open source software is often used in permissionless blockchains. This does not mean that such software is no longer copyright protected but rather that the author(s) has/have decided to allow it to be freely reproduced, adapted et cetera, provided that the users adhere to the terms chosen by the

---

[17] Zhou, Y. et al. (2018), Erays: Reverse Engineering Ethereum's Opaque Smart Contracts, *27th USENIX Security Symposium*, p. 1383.
[18] Articles 5:1 and 3:2 of the Dutch Civil Code.
[19] Section 10(1)(12) of the Dutch Copyright Act.
[20] Section 1(1)(a) of the Dutch Databases (Legal Protection) Act (*Databankenwet*).

author(s) for the open source license. If more than one author has contributed to the development of the blockchain software, then each one of them, in principle, holds the copyright to their own contributions, provided that their own contributions can still be distinguished from the others.[21] The applicable open source license then usually 'harmonises' the terms governing further distribution, adaptation et cetera. As for permissioned blockchains, which are less open, the software they use has quite often been built by just one or a limited number of people and been distributed as closed source software. Others may then use it to participate in the blockchain in question (under the terms of the closed source license), but they themselves are generally not allowed to adapt or distribute it. Nor can they, because the source code needed for that is not released along with the software.

Issues relating to property law are also faced by 'owners' of tokens and cryptocurrencies. A credit in a cryptocurrency does not yet fit into the Dutch statutory system of real rights and proprietary rights. Proprietary rights are usually subdivided into absolute proprietary rights (*absolute vermogensrechten*), effective against anyone, and relative proprietary rights (*relatieve vermogensrechten*), effective against a specific debtor.[22] Tokens, or credit balances on a blockchain, are not covered by either of these categories. They are not legally recognised absolute rights that are effective against anyone. Writers do sometimes make the point that, although not strictly necessary, it might be useful to amend the law in this regard in order to create clarity about the legal status of tokens and cryptocurrencies and thus to define their property law status.[23]

2.2.1. Privacy

The fundamental right to privacy implies the protection of personal data. The most important rules on the protection of personal data in the

---

[21] The situation may be different if, for example, a contribution is made in the context of employment (Section 7 of the Dutch Copyright Act).

[22] Bartels, S.E. and Van Mierlo, A.I.M (2013), *Mr. C. Asser Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 3. Vermogensrecht algemeen*. Deel IV. Algemeen goederenrecht [in Dutch].

[23] Schellekes, M., Tjong Tjin Tai, E., Kaufmann, W., Schemkes, F. and Leenes, R. (2019). Tilburg University, *Blockchain en het recht. Een verkenning van de reguleringsbehoefte*, p. 39.

Netherlands are laid down in the General Data Protection Regulation ("GDPR"). Personal data comprise data that are traceable both directly and indirectly to natural persons. This indirect traceability, in particular, means that a lot of data (e.g., including pseudonyms, location data and online identifiers) qualify as personal data subject to the GDPR. Accordingly, even if no (directly traceable) personal data are recorded on a blockchain, the rules of the GDPR still need to be taken into account. However, those rules are sometimes difficult to apply to blockchain applications.

For instance, the GDPR provides that the person who determines the purposes and means of the processing of personal data is the controller,[24] and he has numerous obligations under the GDPR. The controller must take appropriate technical and organisational measures to protect personal data,[25] instruct processors he or she engages accordingly, carry out a data protection impact assessment[26] if an intended processing operation is likely to result in a high privacy risk,[27] provide detailed information about the personal data processing to data subjects whose data he or she processes[28] and notify data breaches to the supervisory authority (the Dutch Data Protection Authority) as well as to the data subject(s) whose personal data have been breached, depending on the circumstances.[29] In the case of permissionless blockchain applications, it is unclear who should be considered to be the controller(s) and which party/parties are therefore obliged to comply with the obligations set out above. In this regard, the structure of the GDPR seems to be better suited to centralised data storage (with one particular person clearly having decisive control over the purposes and means of processing that data) than to decentralised storage of personal data. Where permissioned blockchain applications are concerned, all the participants are known in principle and

[24] Article 4(7) GDPR.
[25] Article 32(1) GDPR.
[26] Often abbreviated to DPIA or PIA (or, as officially referred to in Dutch law: *gegevensbeschermingseffectbeoordeling*).
[27] Article 35 GDPR.
[28] He or she must also observe all the requirements of Articles 12 – 14 GDPR (duty to inform data subjects).
[29] Articles 33-34 GDPR.

they can agree on the division of the relevant responsibilities among themselves.[30]

Other areas in which the nature of blockchain technology and the rules of the GDPR are awkward bedfellows are the privacy law requirements on data minimisation (the prohibition against processing more personal data than are necessary for the purposes of their processing), data integrity (the obligation to update personal data if they prove to be incorrect/outdated) and storage limitation (prohibition against keeping personal data for any longer than is necessary for the purposes of their processing[31]) versus the characteristic property of the blockchain that the chain of historical data and redundancy of that data (which arises by duplicating it on all nodes) is crucial in order to combat manipulation of that data. This makes it, in principle, impossible to alter/remove historical 'blocks'.[32]

Given this fundamental irreconcilability, the advice often given is not to store any personal data on a blockchain but, at most, to include a reference to personal data stored off-chain. The underlying notion is that, if at any point the personal data stored off-chain are deleted, the undeletable reference to them would not (or no longer) qualify as personal data. A similar reasoning applies in the (alternative) advice to encrypt any personal data stored on a blockchain because, if the key stored off-chain is then removed, that would meet the requirement of removing personal data. Whether such arguments actually stand up under privacy law has not yet been assessed by the courts, nor have the relevant supervisory authorities adopted a position in this regard. Irrespective, we take the view that the on-chain processing of online identifiers (indirectly traceable personal data) is still a form of processing which is relevant under privacy law and which would have to satisfy the requirements imposed by the GDPR.

Last but not least: data export restrictions play an important role under the GDPR in blockchain applications that transcend the borders of the European Economic Area (EEA). Personal data of data subjects who are in the European Union may not be processed outside the EEA unless a statutory

[30] Under Article 26(1) GDPR, such an arrangement must be agreed in certain circumstances.
[31] The 'right to be forgotten' laid down in Article 17 GDPR is a well-known effect of this principle.
[32] This does not include interventions of a hard fork nature.

exception applies. To determine whether, in a specific situation, an exception applies to this data export prohibition and, if so, which one, it is necessary to know which country the data is to be exported to. Given that the identity and location of the relevant parties are often unknown (certainly in the case of permissionless blockchains), accounting for the privacy law requirements of such data exports is practically impossible. All in all, there is still some work to be done in terms of privacy law before blockchains – particularly permissionless ones – can become GDPR-compliant. Amendments to privacy laws and regulations as well as developments in blockchain technology would be helpful in this regard. The table shown below summarises the main problems that still exist in this regard:

Table 1. Clashes between the basic premises of privacy legislation (GDPR) and blockchain technology

GDPR	**Blockchain**
Data minimisation	Redundancy
Controller's duty to provide information	Decentralisation/public/permissionless
Accuracy of data	Un-changeability
Storage limitation	Historical transactions essential
Data-export prohibition	Borderless
Confidentiality	Transparency

2.2.2. Tokens, Cryptocurrencies and Financial Supervision

The advent of the blockchain came hand in hand with the arrival of tokens. Using smart contracts, developers can create and manage tokens, and assign rights to them. The rights associated with tokens may differ.

For instance, asset tokens represent a particular physical product, like gold. Utility tokens give the right to use a certain product or service.[33] Security tokens are investment tokens. A security token holder does not have any ownership rights to the entity they invested in, but instead they are

[33] One example is the Basic Attention Token (BAT), which advertisers can use to buy advertisements. The tokens are distributed among publishers and those viewing the adverts (i.e., consumers). Publishers are given coins for hosting the ads, the consumer for viewing them.

guaranteed a percentage of the profits generated by the entity.[34] Equity tokens function more like a traditional stock asset. Equity holders possess some form of ownership in their investments such as in a project or company; they are considered to be a subgroup of security tokens. Tokens can also be hybrid, i.e., they combine several of these functions.

The nature of the rights attached to tokens is always decisive for the question of what kind of token it is, and whether financial supervision legislation applies to it.[35] If it qualifies as a security (*effect*), then the Dutch Financial Supervision Act (*Wet op het Financieel Toezicht*) ("Wft") applies.[36]

Categorising tokens goes hand in hand with the question of the legal status of the tokens and whether they fall under the Wft or international securities legislation. The Autoriteit Financiële Markten (Dutch Authority for the Financial Markets) and De Nederlandsche Bank (central bank of the Netherlands) have both indicated that, under certain circumstances, the issuance of cryptocurrencies and tokens falls under the scope of the Wft.[37] This is the case if a cryptocurrency or token has features that correspond to 'securities' within the meaning of the Wft. This is relevant if there is a so-called initial coin offering, in which cryptocurrencies and tokens can be issued. Start-ups and existing companies may issue tokens to raise funds through an initial coin offering. Although the majority of tokens issued on an initial coin offering are construed in such a way that they seem to fall outside the scope of the Wft, the authorities may nevertheless consider them to be securities. The authorities have announced that they shall assess initial

[34] Security tokens are issued via a Security Token Offering (STO). One example of a security token is a Blockchain Capital token, or BCAP token. The BCAP token entitles you to a share in Blockchain Capital's profits.

[35] Blemus, S. (2018), *Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide*.

[36] The definition of a 'security' under Section 1:1 of the Dutch Financial Supervision Act is: 1) a negotiable share or other negotiable instrument or right considered equivalent; 2) a negotiable bond or other negotiable debt instrument; or 3) any other negotiable instrument issued by a legal person or corporation by which securities referred to under 1) or 2) may be acquired through exercising the rights attached to this instrument or through conversion, or that can be settled in cash.

[37] https://www.afm.nl/nl-nl/professionals/onderwerpen/ico (consulted on 28 February 2020).

coin offerings to ascertain whether the Wft is applicable, and they have made it known that they intend to monitor this strictly.[38]

Supervisory bodies across the world monitor initial coin offerings and other kinds of token issuances. Among others, the British *Financial Conduct Authority*, the American *Securities and Exchange Commission*, the Chinese *People's Bank of China*, the German *Bundesanstalt für Finanzdienstleistungsaufsicht* and the *Securities and Futures Commission* of Hong Kong warn people about the risks associated with unregulated initial coin offerings. Various national and international supervisory authorities are working together to minimise and eliminate the risks. In Europe, the European Securities and Markets Authority is one of the bodies that is responsible for this. At international level, the International Organization of Securities Commissions is an umbrella alliance of securities regulators that deals with the developments brought about by initial coin offerings.[39]

The Autoriteit Financiële Markten and De Nederlandsche Bank emphasise the need for legislation. They also advocate regulation at international level given the international nature of cryptocurrencies. To this end, they published a joint advisory report – for cryptocurrencies only – for the Dutch Minister of Finance with recommendations for a regulatory framework in 2018.[40] In it, they made several recommendations: a licensing regime should be set up for companies to ensure effective implementation of the revised European anti-money laundering directive. Implementing a licensing system under Money Laundering and Terrorist Financing (Prevention) Act may help to prevent the financial system from being misused for money laundering and terrorist financing.

The second recommendation involves amending the regulations at European level to provide scope for developments in attracting (small-scale) financing with the help of blockchain technology. At the national level, the Autoriteit Financiële Markten and the Nederlandsche Bank advise to amend

---

[38] https://www.afm.nl/nl-nl/professionals/onderwerpen/ico (consulted on 28 February 2020).
[39] https://www.afm.nl/nl-nl/professionals/onderwerpen/ico (consulted on 28 February 2020).
[40] Advice of the Autoriteit Financiële Markten and De Nederlandsche Bank to the Minister of Finance with recommendations for a regulatory framework for crypto's and tokens (December 2018) [in Dutch].

the definition of 'security' to reflect the definition used in European legislation. This will allow the Autoriteit Financiële Markten to include certain cryptocurrencies within the scope of its supervisory perimeter. Amending the definition is, according to the authorities, also desirable in anticipation of potential European consensus on the qualification of certain cryptocurrencies as security under present legislation.

The advisory report also notes that, due to the rapid developments in the cryptocurrency markets, it is unclear what standards need to be set for proportional regulation. The development of these regulations will also take time. The Autoriteit Financiële Markten has, in the meantime, published information on its website about when the Wft applies to the issuance of tokens. If a token can be construed as a security within the meaning of the Wft, then a prospectus approved by the Financial Markets Authority is mandatory.[41]

Apart from the aforementioned advisory report which addresses the need of regulation with respect to cryptocurrencies, the Minister of Finance has announced to investigate whether the definition of securities in the Wft needs to be amended to ensure that the issuance of tokens that constitute securities falls under it as much as possible.[42] This will provide legal certainty to the investor as well as to the providers of tokens that can be considered as securities. The investor then knows that the securities are subject to monitoring and supervision, and it is clear to the provider that a prospectus has to be prepared, and all the other conditions associated with the duty to provide a prospectus must be met. The Minister of Finance also intends to investigate the efficiency benefits of blockchain technology for payment and securities transactions.[43]

2.2.3. Applicable Law/Jurisdiction

Blockchain applications are ideal for cross-border use. That said, if there is a dispute involving a blockchain, this raises the question as to which

[41] Section 5:2 of the Financial Supervision Act, unless it is subject to an exception or exemption provided for by law.
[42] Parliamentary Papers II 2018-2019, 32013, no. 201.
[43] Parliamentary Papers II 2018-2019, 32013, no. 200.

national law applies, and which court is competent to hear the dispute. There are, however, no easy answers to the questions on the applicable law and which court is competent to hear the dispute. How the blockchain is set up is a determining factor. In the same way that parties to more traditional (cross-border) contracts can agree on the law applicable between them (‘*rechtskeuze’*) and the competent court (‘*forumkeuze’*), it is possible to set conditions for joining blockchains. The accession contract or the general terms and conditions applicable to the contract may state which law is applicable and which court or authority is competent to hear the dispute. Ethereum, among others, has deliberately opted for this:

> ‘All matters relating to the Websites and these Terms of Use and any dispute or claim arising therefrom or related thereto (in each case, including non-contractual disputes or claims), shall be governed by and construed in accordance with the internal laws of Switzerland without giving effect to any choice or conflict of law provision or rule (whether of Switzerland or any other jurisdiction).
>
> Any legal suit, action or proceeding arising out of, or related to, these Terms of Use or the Websites shall be instituted exclusively in the Switzerland in the Kanton of Zug although we retain the right to bring any suit, action or proceeding against you for breach of these Terms of Use in your country of residence or any other relevant country. You waive any and all objections to the exercise of jurisdiction over you by such courts and to venue in such courts.’[44]

If no explicit choice of law and forum has been agreed in the legal relationship between the users of a blockchain application, the question of which law applies and which court has jurisdiction in international disputes will have to be answered on the basis of the treaties or EU regulations

[44] https://ethereum.org/terms-of-use/ (consulted on 28 February 2020). ‘Website’ is defined as: The following terms and conditions, together with any documents they expressly incorporate by reference (collectively, these ‘Terms of Use’), govern your access to and use of ethereum.org, including any content, functionality and services offered on or through ethereum.org, ethereumfoundation.org and blog.ethereum.org.

applicable between the countries concerned.[45] In the absence of such, national private international law, like that laid down in the Netherlands in the Dutch Code of Civil Procedure and Book 10 of the Dutch Civil Code, will apply. In practice determining with any certainty which law applies and/or which court has jurisdiction in a specific situation often proves to be a complicated business. Anyone seeking certainty in advance is better off agreeing on a choice of law and a choice of forum. This is not difficult in permissioned blockchain applications. In permissionless applications, it can be more difficult due to the lack of a legal relationship between the parties involved in that blockchain (see the 'Contracts' section discussed previously).

3. Real-Life Examples

Several areas of law may play a role in the application of blockchain technology. To familiarise you with some examples of the possible legal ramifications of blockchain applications, two real-life examples are elaborated below. First an example of a permissioned application in healthcare (Mijn Zorg Log (i.e., My Healthcare Log)) is discussed, followed by an example of a permissionless application using cryptocurrencies. We would like to point out that other laws and regulations (including sector-specific ones) may also apply to these examples. This legislation is not covered in the selection of legal areas set out below.

3.1. Mijn Zorg Log

> "Using Mijn Zorg Log suits our times, it is convenient and easy. I'd love to use it in my work right now. And if it would be possible in the future, with the mother's consent, to share patient information too, for

[45] One example of this is the Rome I Regulation. This is the European regulation that governs the applicable law in international agreements (contracts) concluded between parties established in the European Union.

example, with the obstetrician, GP or the baby clinic, that would be ideal for my work. Then everyone concerned with the handover would have the same information."[46]

3.1.1. Introduction

The blockchain application, Mijn Zorg Log, is an example of a blockchain pilot for the exchange of digital information in the case of long-term care. In a first practical trial, the Dutch National Healthcare Institute (*Zorginstituut Nederland*) has investigated whether and to what extent the use of blockchain technology could be applied to maternity care administrative processes. More specifically, blockchain technology was used for maternity care time recording.

The organisations involved in the pilot project are the Dutch National Healthcare Institute, healthcare insurer VGZ, three maternity care providers (LiemersCare, South Gelderland and VDA), software developer Ledger Leopard, around 30 maternity nurses and 33 mothers.

The traditional method of recording hours spent on maternity care was as follows. The maternity nurse noted the number of hours of maternity care provided each day. The mother then signed off the records. If there was a discussion about the actual number of hours of maternity care provided, the final outcome was written on the timesheet, which the mother would then sign. After the maternity period, the maternity nurse took the signed timesheets and sent them on to the maternity care provider. The maternity care provider then checked the timesheets and entered the information into its own system. The hours of maternity care provided were then submitted to the healthcare insurer. After the healthcare insurer had checked the sheets, the maternity care provider would then be paid for the hours of service.

During the practical trials with the Mijn Zorg Log blockchain application, the administration process was as follows. The mother was given access to her own blockchain wallet in the Mijn Zorg Log dashboard. The mother then configured the necessary permissions. In other words: she had control over who got access to which data. When providing maternity

[46] Quote from a maternity nurse at a maternity care home (South Gelderland) who participated in the blockchain pilot.

care, the maternity nurse could immediately enter the hours of service in the Mijn Zorg Log application. If the mother didn't agree with the hours entered, then she could reject the transaction, stating her reasons. In that case, the maternity nurse would then correct the number of hours, and the mother would then approve them again. At the end of the maternity period – but in fact also on a daily basis – it was immediately clear to everyone concerned how many (approved) hours of service the maternity nurse had provided.

The trial showed that time recording through Mijn Zorg Log was more transparent and more efficient. Working with Mijn Zorg Log made it possible for everyone involved in maternity care to reconfigure the administrative process. By accessing the Mijn Zorg Log application, there was one reality for all those involved. The result of the blockchain trial was that using Mijn Zorg Log significantly lightened the administrative burden for all those involved.[47]

3.1.2. Contracts

Smart contracts were used in Mijn Zorg Log for, among other things, submitting claims and invoices. Transactions were validated through the consensus mechanism 'proof of authority'. The contract terms with respect to the manner of validation of transactions, in this case proof of authority, had been laid down in advance between the parties involved.[48]

Implementing a smart contract can be done in two ways: through deterministic contracts and non-deterministic contracts. In the first case, running the software code is not dependent on information from outside the blockchain to implement a contract. All the requisite information is already stored in the blockchain. In the second case, information from outside the blockchain is needed to trigger the implementation of the contract. The provider of this external information is called an 'oracle'.

In the Mijn Zorg Log case, it was always the parties involved who made the implementation of the smart contracts possible. The implementation of

---

[47] https://istandaarden.nl/izo/innovaties/blockchain-mijn-zorg-log (consulted on 28 February 2020) [in Dutch].

[48] This is described in Chapter 1 of the report entitled '*Praktijkproef blockchain kraamzorg met Mijn Zorg Log'* (Practical trial of blockchain maternity care using My Healthcare Log) of 14 June 2018, p. 8 and further [in Dutch].

the contract, for instance claiming expenses after the hours had been sent on to the insurer, required information from oracles outside the blockchain. It is evident that this process requires those involved to provide the correct input. Otherwise a smart contract would be reduced to an efficient and effective way of carrying out a defective or fraudulent process. An incorrect outcome may harm one of the parties involved. On the other hand, an error in the code may result in a smart contract being implemented incorrectly. To avoid debate, the question of who is liable for damages due to incorrect coding can be contractually arranged in advance.

For instance, identifying the legal issues involved in the Mijn Zorg Log led to the preparation of at least the following documents prior to the practical trial: a cooperation contract (‘*samenwerkingsovereenkomst’*), a data processing and sub-processing contract (‘*(sub)verwerker-sovereenkomst’*) (see further in this section) and a conditions of use contract (‘*gebruiksvoorwaarden’*).[49]

3.1.3. Intellectual Property

Ledger Leopard developed the Mijn Zorg Log blockchain software based on a platform derived from Ethereum.[50] Ethereum is free and open software, although it is not clear which specific permissive open source licence will apply to the Ethereum core:

> ‘The core of Ethereum will be released under the most liberal of licenses. (…) In this way, while we have not arrived at a final license, we expect to select one of the MIT license, the MPL license or the LGPL license. (…) In this way, the core of Ethereum, be it C++ or Go, will be available for use in any commercial environment, closed or open source.’[51]

[49] This is decribed in the report ‘Praktijkproef blockchain kraamzorg met Mijn Zorg Log’ (Practical trial of blockchain maternity care using My Healthcare Log) of 14 June 2018, p. 18 and further [in Dutch].

[50] This is decribed in the report ‘Praktijkproef blockchain kraamzorg met Mijn Zorg Log’ (Practical trial of blockchain maternity care using My Healthcare Log) of 14 June 2018, p. 27 [in Dutch].

[51] https://github.com/ethereum/wiki/wiki/licensing (consulted on 1 March 2020).

Parties that develop their own applications based on this core therefore have the option of distributing their copyright to that application under a different license, which may also be a closed-source license. Ledger Leopard also seems to be doing this, as evidenced by the arrangement in Article 11.1 of its general terms and conditions:

> 'The Intellectual Property Rights associated with the Platform, Ledger Leopard Software and the rights related to the results of the Services are vested exclusively in Ledger Leopard and/or its licensor(s). The Client will only acquire the rights and licenses granted to it under the Agreement.'

Unless arrangements are made that deviate from these general terms and conditions, the parties using Mijn Zorg Log use the software on the basis of a license obtained from Ledger Leopard but they do not become the copyright holder(s) of this software.

Intellectual property rights may also be attached to the data stored in the blockchain. However, the data registered in Mijn Zorg Log (such as the number of hours of maternity care provided by X to Y) is of such a factual nature that it will not easily be construed as being original in nature or bearing the personal imprint of the maker. Copyright protection for that kind of data does not therefore seem to be relevant.

Database protection under the law does not appear to be relevant either, since it is not possible to designate a single party as having made a substantial investment in qualitative or quantitative terms in the acquisition, control or presentation of the content. Indeed, the content of the Mijn Zorg Log blockchain is the result of various parties entering data. It also has to be borne in mind that there may be no protection due to the so-called spin-off principle. Put briefly, this principle means that there is no database protection if the investment in acquiring, managing and/or presenting the data has to be carried out in the context of the normal business operations of the 'producer' of the database.

Since there appears to be neither copyright nor database protection on the data in this blockchain, and – as explained in the previous section – data does not qualify as an object which can be owned, our interim conclusion on

this point is that, from a legal perspective, no one is the 'owner' or 'rightholder' of the data in this blockchain application.

3.1.4. Privacy

Given that Mijn Zorg Log is used in a context in which data relating to health is processed (in terms of the GDPR, this qualifies as 'special personal data', which is subject to a stricter regime for processing),[52] responsibility under privacy law for the use of Mijn Zorg Log is a critical matter. It is no coincidence that extensive research has been carried out into this aspect, and a great deal of effort has been spent on trying to set-up this application in compliance with privacy legislation.[53]

Partly for the privacy law reasons set out in Section 2 of this chapter, Mijn Zorg Log was set up as a permissioned blockchain. In this way, agreements could be reached between the parties about, inter alia, the division of responsibility in the processing of personal data in the context of Mijn Zorg Log, for instance designating the party responsible for reporting data breaches to the Dutch Data Protection Authority. In order to meet the data minimisation obligation, it was decided to place as little personal data as possible on chain. In the practical trial, the blockchain only included hours of maternity care, with a digital key to the people involved. However, this still concerns (special) personal data, which means that, for instance, the data storage limitation principle would also have to be met (data should not be stored for longer than is necessary for the purpose for which it is being processed) and requests from data subjects to 'be forgotten' would have to be granted. In the Mijn Zorg Log set-up, an attempt was made to address this by, among other things, encrypting the personal data stored on chain based on the notion that the associated (off chain) key could be deleted if

---

[52] Article 9 GDPR.

[53] This is handled in great detail in Chapter 3 of the report entitled 'Praktijkproef blockchain kraamzorg met Mijn Zorg Log' (Practical trial of blockchain maternity care using My Healthcare Log) of 14 June 2018 and in the underlying report by Pels Rijcken commissioned by the Dutch National Healthcare Institute entitled 'Blockchain in de zorg in relatie tot de AVG – Een onderzoek naar de wijze waarop het gebruik van blockchain in de zorg in overeenstemming kan worden gebracht met de AVG' (Blockchain in healthcare and the GDPR – Research into how the use of blockchain in healthcare can be made GDPR compliant).

necessary. As indicated in the previous section of this chapter – and as is acknowledged in the final report on Mijn Zorg Log – it is doubtful whether this complies with the storage limitation related obligations under the GDPR. As long as there is a hypothetical possibility that the encrypted personal data can be retrieved by, for example, a person with malicious intent – and who knows, future technologies may make such decryption easier – in our opinion, this encrypted data continues to qualify as personal data within the meaning of the GDPR and therefore Mijn Zorg Log did not comply with the storage limitation principle. That said, the entire blockchain can be deleted – and this option is also referred to in the aforementioned final report – but outside the context of a pilot study this is not really a realistic/workable option.

The following is also worth mentioning with respect to this example:

- it seems as though the GDPR does not apply to the processing of personal data by mothers on the Mijn Zorg Log blockchain, because the GDPR does not apply to the processing of personal data by natural persons when carrying out a purely personal or household activity (Article 2(2) GDPR);[54]
- parties that do not add data to the blockchain (such as the Dutch National Healthcare Institute and Ledger Leopard) but only do processing for the controller(s) (validating data for instance) are considered in Mijn Zorg Log to be processors (with which contracts within the meaning of Article 28 of the GDPR have to be concluded), and parties that do add data to the blockchain (such as maternity care providers) are considered to be controllers, who make mutual arrangements on the division of their responsibilities within the meaning of Article 26 GDPR;
- that the Dutch National Healthcare Institute conducted a data protection impact assessment (DPIA) within the meaning of Article 35 of the GDPR prior to collecting the data. That this GDPR obligation was carried out is, of course, commendable. What is

[54] Also see the aforementioned report by Pels Rijcken, p. 36.

striking, however, is that in the Mijn Zorg Log the Dutch National Healthcare Institute was designated as a processor, whereas carrying out a data protection impact assessment is an obligation for the controller.[55]

3.1.5. Applicable Law/Jurisdiction

As previously discussed, the normal rules of private (international) law can be applied to determine which legal system is applicable and which court is competent to hear a dispute. If it concerns a permissioned blockchain like Mijn Zorg Log, however, the sensible thing would be to avoid discussion by including a clause in a contract or in general terms and conditions that lays down which law is applicable and which court is competent to hear disputes. In this example, however, it hardly seems relevant given that all those involved in this permissioned blockchain are based in the Netherlands.

3.1.6. Sector-Specific Legislation

Mijn Zorg Log is a real-life example involving the recording of healthcare data. There may therefore also be legal requirements under, for example, the Dutch Social Support Act [*Wet maatschappelijke ondersteuning*], the Dutch Long-Term Care Act [*Wet langdurige zorg*], the Dutch Youth Act [*Jeugdwet*] and/or the Dutch Healthcare Insurance Act [*Zorgverzekeringswet*]. This analysis does not discuss the consequences of sector-specific regulations.

3.2. Cryptocurrencies

> 'Cryptocurrencies or bitcoins, or anything like that, are not really currencies – they are assets. A euro is a euro – today, tomorrow, in a month – it's always a euro. And the ECB is behind the euro. Who is behind the cryptocurrencies? So they are very, very risky assets.'[56]

[55] Pursuant to Article 28(3)(f) GDPR, the processor is only obliged to provide assistance in this regard.

[56] Quote of Mario Draghi, President of the European Central Bank during the European Central Bank Youth Dialogue.

3.2.1. Introduction

Cryptocurrencies are (considered to be) the new digital currency. Cryptocurrencies represent a certain value which depends on the value that the participants in the network assign to the cryptocurrency. Unlike traditional currency units, cryptocurrencies are not state-created or regulated units of account. Cryptocurrencies are purely private creations.

In 2009, Satoshi Nakamoto believed that a peer-to-peer cash system was called for. Nakomoto succeeded in creating an electronic payment system based on cryptographic proof allowing two parties to transact directly with each other without the need of a trusted third party. This cryptographic peer-to-peer cash system is better known as the Bitcoin. Other well-known examples of cryptocurrencies are, for example, Ether and Ripple. Facebook tried to introduce its own cryptocurrency: the 'Libra', but this digital currency was not generally (and warmly) embraced. The reason for this was that government authorities, banking authorities and privacy activists feared that the Libra would give ample scope for illegal activities such as money laundering, the financing of weapons and the misuse of personal data. Despite this, according to the International Organization of Securities Commissions (IOSCO), the worldwide alliance of supervisory bodies, the Libra may fall under existing legislation, and thus be subject to the supervision of (national) authorities:

> "Our analysis has shown that so-called "stablecoins" can include features that are typical of regulated securities. This means IOSCO Principles and Standards may apply to stablecoins depending on how they are structured, including those related to disclosure, registration, reporting and liability for sponsors and distributors."[57]

This position taken by IOSCO did not stop several EU Member States from working on measures to prohibit the arrival of the Libra.[58] The Minister

[57] Alder, A., Chair of IOSCO.

[58] Veuger, J., Libra and Anxiety Rhetoric: fear to be Eaten. Res Dev Material Sci. 12(2).RDMS.000782.2019. DOI: 10.31031/RDMS.2019.12.000782.

of Finance also indicated[59] – as mentioned in section 2 – that he is preparing a regulatory framework that will impose on, among other things, stricter requirements for advertisements for risky financial products.[60] The reason for this is that cryptocurrencies are a new phenomenon, one for which the current supervisory and regulatory frameworks are not yet equipped.[61]

Back to bitcoin. Bitcoins can be acquired on the Bitcoin blockchain according to the 'proof of work' concept. This means that bitcoin transactions can be carried out and verified using cryptography (i.e., miners). Using the bitcoin blockchain thus makes it possible to transfer bitcoins from one party to another without the intervention of a third party, like a banking institution. To verify the transaction, the miners must solve a mathematical puzzle. The first miner who solves the puzzle is given a reward in the form of bitcoins. In the proof of work concept, the presence of miners on a blockchain means that there is no central organisation responsible for issuing, transferring and validating transactions. Those that do this are the participants/miners themselves.

Cryptocurrencies must be distinguished from the tokens mentioned above. Whereas cryptocurrencies are defined by a blockchain protocol, tokens are defined by smart contracts.[62]

3.2.2. Legal Status: Cryptocurrencies from the Perspective of Tax Law and Civil Law

Bitcoins have been used to 'make payments' since 2010. This is interesting when one considers that the legal status of the bitcoin – and other cryptocurrencies – under Dutch property law is not yet clear, let alone that it actually constitutes a payment method.

---

[59] Letter from the Minister of Finance Hoekstra of 8 March 2018, '*Kamerbrief over de ontwikkelingen rondom cryptovaluta: appreciatie ontwikkelingen cryptovaluta',* (appreciation trends in cryptocurrencies) [in Dutch].

[60] For instance bitcoin futures and binary options.

[61] Parliamentary paper on Financial Markets (Amendment) Act 2018 (2017 to 2018), 34859 no. 3.

[62] Nannings, M.A.R., (2018), *Regulering van Initial Coin Offerings: een raamwerk voor regulering door de kwalificatie van tokens als effect*, p. 34 [in Dutch].
The https://coinmarketcap.com/ website can be consulted to check whether in a specific case it is a token or a cryptocurrency.

The tax authorities have argued that the bitcoin is a means of payment that should be equated with money, and therefore subject to capital gains tax on the value. Taxpayers are obliged to declare the value of their cryptocurrencies at the value that can be assigned to them in the course of trade each year.

From a civil law perspective, experts hold a different view. On 14 May 2014, the Overijssel District Court ruled that bitcoins do not qualify as money in the conventional sense within the meaning of Article 6:112 of the Dutch Civil Code. The court instead held that they are a means of exchange.[63] The court arrived at that opinion because the bitcoin is not legal tender. That said, the court did find that, with the 'conventional money' provision, the legislature deliberately took account of the fact that a means of payment does not necessarily have to originate from a state government. However, because as it stands now bitcoins are not yet legal tender in the Netherlands, and because the Minister of Finance believes that the bitcoin is not money within the meaning of the Wft and therefore bitcoin cannot be tolerated as a means of payment, the court found that bitcoins are not conventional money.

The European Central Bank has also expressed an opinion about whether bitcoins can be considered 'money'. Like the Minister of Finance, the European Central Bank is of the opinion that cryptocurrencies, such as the bitcoin, cannot be regarded as money, "the ECB does not regard virtual currencies, such as Bitcoin, as full forms of money as defined in economic literature. Virtual currency is also not money or currency from a legal perspective."

In the Netherlands, property law is structured under the law as a closed system. Pursuant to Article 3:1 of the Dutch Civil Code, property law only applies to two types of property: objects and proprietary rights. If bitcoin, and cryptocurrencies in general, do not fall within this definition, then Dutch property law does not apply to them.

[63] Overijssel District Court 14 May 2014, ECLI:NL:RBOVE:2014:2667.

Does bitcoin qualify as a proprietary right? This question is very pertinent in practice, for instance for determining whether a claim in bitcoins can serve as a second creditor's claim when filing for bankruptcy.[64]

The question of whether bitcoin can be regarded as a proprietary right has already been answered in the affirmative by a lower court in the Amsterdam district in 2018.[65] Bitcoin represents value and is transferable. The commitment to pay in bitcoin can be considered to be an obligation to pay. This means that is has features that are consistent with a proprietary right. The court also found that a claim in bitcoins can serve as a second creditor's claim when filing for bankruptcy. It is argued in the literature that classifying cryptocurrencies as proprietary rights is not that simple. The rationale underlying this is that a proprietary right is a personal right, against which a debt is owed. This is not the case with bitcoin. A bitcoin is a series of encrypted codes with a specific market value. A bitcoin does not give the owner the right to the value that the bitcoin represents; instead it has that value itself.[66]

The above leads to the conclusion that it is not entirely legally correct to refer to 'owners' of bitcoins. It is more correct to speak of a possessor of bitcoins who is therefore the owner of a proprietary right. We would also like to point out that the status of cryptocurrencies is currently derived from the case law of lower courts. The Dutch Supreme Court has not yet delivered an opinion on this matter.

Some crypto service providers will soon be obliged to register with De Nederlandsche Bank, before they can offer their services in the Netherlands. These include organisations that offer professional or commercial custodial wallets, and parties that offer professional or commercial services for exchanging virtual currencies and fiat currencies.[67] This obligation to

---

[64] In the Netherlands, the bankruptcy of a person or company can only be filed if there is at least one enforceable claim and a second creditor's claim and the debtor has stopped paying.

[65] Amsterdam District Court 14 February 2018, ECLI:NL:RBAMS:2018:869.

[66] Rank, W.A.K. (2015), *Bitcoins: civielrechtelijke en toezichtrechtelijke aspecten. Bitcoins civiele en fiscale aspecten in beeld*, p. 36 [in Dutch].

[67] Fiat money is money issued by a government, like the euro. Unlike cryptocurrencies, the government can influence the value of fiat money. For instance, the government can print money, put more money into circulation or carry out other actions that may change the relationship between the supply and demand for fiat money.

register follows from the impending integrity supervision of (certain) providers of crypto services.[68] Later in this section we discuss the forthcoming legislation in greater detail.

3.2.3. Intellectual Property

The bitcoin core software is subject to the MIT open source license. This is called a permissive license, which offers users ample freedom to adjust the software at their discretion and to distribute it (also commercially) under different terms and conditions. The only obligation in exchange for this is to include the copyright notice and the permission notice. Finally, the license contains a huge exclusion of liability for damage caused by the use of the software. The full text of this clear-cut license reads as follows:[69]

> "The MIT License (MIT)
> Copyright (c) 2009-2020 The Bitcoin Core developers
> Copyright (c) 2009-2020 Bitcoin Developers
>
> Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
>
> "The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
>
> THE SOFTWARE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE

[68] The European Anti-Money Laundering Directive (AMLD 5) and its implementation in the Dutch Money Laundering and Terrorist Financing (Prevention) Act (*Wet ter voorkoming van witwassen en financieren van terrorisme*).

[69] https://github.com/bitcoin/bitcoin/blob/master/COPYING (consulted on 1 March 2020).

> AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE."

The blockchain generated by the bitcoin software (put simply: the ever-growing list of bitcoin transactions[70]) is not subject to any copyright, because the format is technically defined and therefore it doesn't seem to have an original character/the personal imprint of the maker. In our opinion, there is also no one producer who has made a substantial investment in the creation of the database of bitcoin transactions, but rather an extraordinarily large number of independent parties who add a block to the ledger with each transaction (see also the reasoning in the real-life example of Mijn Zorg Log), as a result of which protection under database law does not seem to be applicable.

3.2.4. Privacy

From a privacy-law perspective, the Bitcoin blockchain is a textbook example of how permissionless blockchain applications clash with the requirements of the GDPR. The transaction data on the Bitcoin blockchain contain data that, in combination with other information (i.e., indirectly), can be traced back to natural persons[71] and this therefore falls within the scope of the GDPR.[72] First of all, since there is (deliberately) no central point of contact/responsible organisation in the bitcoin community, it is not evident who should be designated as the controller(s) for these personal data. It is often assumed that the collective of users, nodes and miners are joint

---

[70] When this legal analysis was written, the size was approximately 250Gb; see https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/forunderlying data.

[71] Although a lot of advice can be found at https://bitcoin.org/nl/bescherm-uw-privacy (consulted on 1 March 2020) on how to make bitcoin address traceability more difficult, for example by never using the same bitcoin address more than once.

[72] On this point - similar to the reasoning in the Mijn Zorg Log example - an exception may also be made for natural persons who perform bitcoin transactions exclusively in the course of a purely personal or household activity (Article 2(2) GDPR).

controllers[73], as none of them has individual control of the purpose and the (technical) means used, but changes therein can only be made with sufficient consensus[74]. This would mean that all these parties would have to jointly adopt an arrangement on their mutual division of responsibilities as prescribed in Article 26 of the GDPR. As these parties generally do not (or cannot) know each other, and as there is no bitcoin pre-contract to which all parties have to conform before joining this collective, this is a rather unrealistic scenario and conflicts with this part of the GDPR are likely to occur.

An additional problem is the international character of the processing of personal data on the Bitcoin blockchain. As explained in section 2 of this chapter, the data export prohibition in the GDPR means that the processing, outside the European Economic Area, of personal data of data subjects situated within the European Union is not permitted, unless an exception applies. In order to be able to determine whether an exception to this data export prohibition applies in a specific situation (and which one), you need to know the country to which the data will be exported. Because - on the permissionless Bitcoin blockchain - the identity and location of the data subject is usually unknown, it is virtually impossible to account for the data export that is unavoidable in such a bitcoin application.

In addition to the aforementioned examples of the problematic marriage between the GDPR and permissionless blockchain applications, we would like to mention a few more:

- the conflict with the storage limitation principle (the bitcoin address of a user and his balance and transactions are and remain publicly accessible on the Bitcoin blockchain),

[73] Although on this point it could also be argued that parties that do not add transactions but merely - and on behalf of the controller(s) - engage in storing and validating transactions qualify as processors, this reasoning is problematic (in any case in permissionless blockchains) in view of the absence of an assignment / processing agreement between these parties and the controller(s), as a result of which these 'processors' could still be regarded as data controllers pursuant to Article 28(10) GDPR.

[74] See for example Buocz et al. (2019), Bitcoin and the GDPR: Allocating responsibility in distributed networks, Computer Law & Security Report, Elsevier.

- the conflict with the data minimisation principle (the redundancy inherent in a blockchain is difficult to reconcile with the prohibition to process personal data if that is not necessary for the purpose),[75]
- the impossibility of removing this information from the blockchain generated by the bitcoin software without, practically speaking, unacceptable consequences, and
- the lack of clarity (in the absence of the aforementioned arrangement under Article 26 of the Regulation) as to who should be responsible for reporting data breaches, for carrying out a Data Protection Impact Assessments (DPIA) if mandatory and for informing data subjects as required by Articles 13/14 GDPR.

In view of the above, it can be concluded that the set-up of the GDPR leaves something to be desired, to put it mildly, in the case of distributed storage of personal data.

3.2.5. Money Laundering and Terrorist Financing (Prevention) Act (Wwft)

On 10 December 2019, the House of Representatives (*Tweede Kamer*) adopted the implementation act of the Wwft. This legislative proposal regulates that individuals, legal entities or companies that provide one or more specific services fall within the scope of the Wwft.

As of the moment the Wwft enters into force, two types of providers of services involving virtual currencies must register with De Nederlandsche Bank: services for the exchange between virtual and fiduciary currencies, and providers of custodian wallets that provide services to safeguard private cryptographic keys on behalf of their customers, to hold, store and transfer virtual currencies. The duty to register only applies to parties that provide these services in a professional capacity or on a commercial basis in or from the Netherlands.

[75] After all, there are alternative means/techniques available for carrying out financial transactions that are less invasive of privacy.

As a result, these parties now have to conduct client screening, monitor transactions and report unusual transactions to the Financial Intelligence Unit (FIU). If the crypto service provider does not comply with the obligations ensuing from the Wwft, De Nederlandsche Bank may cancel its registration. In that case, the crypto service provider may no longer carry out its activities. In addition, De Nederlandsche Bank has the authority to impose (substantial) administrative penalties. Lastly, the violation of sanction regulations[76] may lead to criminal enforcement by the Public Prosecutor's Office.

At the moment, it is still unclear within which term crypto service providers will have to comply with the new regulations. At the time this analysis was written, the legislative proposal still had to be ratified by the Senate (*Eerste Kamer*). Nevertheless, De Nederlandsche Bank has stated in a newsletter that it is already possible to carry out preparatory work and to submit a registration request via De Nederlandsche Bank's Digital Supervision Portal. However, there is no need to rush, as De Nederlandsche Bank has indicated that it will not be able to formally process the registration request until the legislation comes into force.[77] If, as a crypto service provider, you would like to study the registration conditions anyway, you will find a detailed explanation of the registration form on the website of De Nederlandsche Bank (in Dutch).[78]

The implementation act, and the ensuing obligations, prompted several crypto service providers to take action. The trading platform Deribit for example, has now chosen to transfer all its trading activities to DRB Panama Inc., a subsidiary of the Dutch company headquartered in Panama.[79]

---

[76] The obligation to register ensues from both the Wwft and the Sanctions Act 1977 (*Sanctiewet 1977*).

[77] Newsletter (11 Februari 2020), De Nederlandsche Bank for crypto service providers ., section "Practical information on registration",.

[78] https://www.toezicht.dnb.nl/2/50-237975.jsp (consulted on 2 March 2020).

[79] NOS Nieuws (10 January 2020), *Crypto bedrijf vertrekt door nieuwe regels: "mogelijk volgen er meer*" (Crypto company leaves because of new rules: 'more may follow' [in Dutch].

3.2.6. Applicable Law/Jurisdiction

As indicated earlier in this chapter, in an international setting, it may be unclear in the event of a dispute which law is applicable and which authority has jurisdiction to hear the dispute. However, developers can avoid such discussions. For example by having users, when joining a blockchain, explicitly enter into a contract that designates a competent court and the applicable law. The developers of Ethereum chose to do so. In the event of a dispute concerning the Ethereum blockchain, it is therefore easy to answer the question of which law is applicable and which authority has jurisdiction to hear the case. After all, the terms of use state that Swiss law applies, and that the court in Zug has jurisdiction to hear disputes.[80]

In disputes and discussions regarding transactions on the Bitcoin blockchain, the question of which law applies and which court has jurisdiction to hear the dispute is less straightforward to answer as no terms of use have been declared applicable. In the case of disputes, the applicable law and competent authority will have to be determined based on treaties and national rules of private international law.[81]

CONCLUSION

The advent of the blockchain is keeping various authorities busy. For example, the Ministry of Security and Justice (*Ministerie van Veiligheid en Justitie*) has commissioned an exploratory study into the social and ethical consequences of blockchain.[82] The European Union Blockchain Observatory & Forum – a European Commission initiative to accelerate blockchain innovation and the development of the blockchain ecosystem

[80] https://ethereum.org/terms-of-use/ (consulted on 5 March 2020).

[81] Incidentally, in the event of disputes about bitcoin transactions, this complication should be distinguished from another complication which is that, due to the direct untraceability resulting from the use of bitcoin addresses, without additional information it will often be difficult to determine which person was behind which transaction and in which country that person lives / is established.

[82] Schellekes, M., Tjong Tjin Tai, E., Kaufmann, W., Schemkes. F. and Leenes, R. (2019), *Report: Exploratory study into the social and ethical consequences of the Blockchain and how the government could/should deal with them.*

within the European Union – published a report in 2018 on Blockchain and the GDPR.[83] In 2019 a thematic report was published by the European Union Blockchain Observatory & Forum with respect to the legal and regulatory framework of blockchains and smart contracts.[84]

Although blockchain technology gives rise to numerous legal questions, it seems that some of the questions can be answered through existing legislation. The mere fact that there is a legal question, does not necessarily mean that the law needs to be amended. Nevertheless, at this point, there is no specific regulatory framework for blockchain and cryptocurrencies. It would be of benefit to legal certainty for the property law status of cryptocurrencies and tokens to be clarified, and the concept of 'security' within the meaning of the Wft to be further defined. It is also desirable to amend or clarify the privacy law rules that apply in the case of the decentralised storage of personal data, as the GDPR is based on the assumption that (a) clear (central) controller(s) can be designated for the processing of personal data, which is not the case with permissionless blockchain applications such as Bitcoin.

We also note that several Dutch authorities, such as De Nederlandsche Bank and the Autoriteit Financiële Markten, are open to discussion on the nature of certain products and/or services that function on the blockchain. The InnovationHub is a joint venture between the Autoriteit Financiële Markten and De Nederlandsche Bank, to provide support for questions about supervision and related regulations concerning innovative financial products or services. The InnovationHub acts as a sparring partner, and can provide guidance on possible supervision issues with respect to blockchain applications. To date, the Dutch Data Protection Authority has been reticent about providing information on how to deal with the requirements ensuing from the GDPR in permissionless blockchain applications.[85]

---

[83] Lyons, T., Courcelas, L. and Timsit, K. Report (2018), *Blockchain Union Observatory & Forum, 'Blockchain and the GDPR'*.

[84] Lyons, T., Courcelas, L. and Timsit, K. Report (2019), *Blockchain Union Observatory & Forum, 'Legal and Regulatory Framework of Blockchains and Smart Contracts'*.

[85] On the website www.autoriteitpersoonsgegevens.nl only one result can be found - at the time of writing - from the search term 'blockchain' and this one result refers to the 2018 annual report of the European Data Protection Board (EDPB) announcing the intention to investigate technologies such as blockchain in 2019 or 2020.

DISCLAIMER

This analysis has been written by the authors with the utmost care. Nevertheless, when reading it you should take account of the fact that the subject is still uncertain territory and that the future will show what the actual legal implications of the blockchain will be. You cannot derive any rights from the content of this analysis. Due to changing legislation and regulations at national and international level, it is possible that the text is not up to date when you read it.

Moreover, the scope of the legal consequences will always depend on the sector in which the blockchain application is implemented. Sector-specific legislation may apply. Judicial interpretations cited in this chapter have mainly been given by lower courts. When this analysis was written, the Dutch Supreme Court had not yet had the opportunity to comment on the legal status of cryptocurrencies and/or tokens and acts that take place on the blockchain. It goes without saying that we will keep a close eye on these developments for you.

REFERENCES

Autoriteit Financiële Markten (n.d.), *Initial coin offerings (ICO's): grote risico's*, Amsterdam: Autoriteit Financiële Markten.

Bartels, S.E. and Van Mierlo, A.I.M (2013), Mr. C. *Asser Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 3. Vermogensrecht algemeen. Deel IV. Algemeen goederenrecht.* [*Asser Manual for the Practice of Dutch Civil Law. 3. Property law in general. Part IV. General property law.*]

Beerepoot, Y.S. (2018), *Blockchain unchained: gevolgen van blockchain en cryptocurrency voor de faillissementspraktijk*, Tijdschrift voor Insolventierecht 2018/34, Deventer: Wolters Kluwer. [*Blockchain*

unchained: consequences of blockchain and cryptocurrency for bankruptcy practice]

Blemus, S. (2018), *Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide*, Social Science Research Network (SSRN).

Buocz et al. (2019), Bitcoin and the GDPR: Allocating responsibility in distributed networks, *Computer Law & Security Report*. Amsterdam: Elsevier.

Felix et al. (2018), *Praktijkproef blockchain kraamzorg met Mijn Zorg Log* [*Practical trial of blockchain maternity care using My Healthcare Log*] of 14 June 2018.

De Nederlandsche Bank (2018), *Crypto's, aanbevelingen voor een regelgevend kader*, Amsterdam, De Nederlandsche Bank N.V. [*Cryptos, recommendations for a regulatory framework]*

De Nederlandsche Bank (2020), *Informatie registratie aanbieders van cryptodiensten*, Amsterdam, De Nederlandsche Bank N.V. [*Information registration providers of crypto services*]

De Vries, E. (2019), *Smart Contracts: een keten van vertrouwen reikend tot in de fysieke wereld*, Nederlands Tijdschrift voor Burgerlijk recht, Deventer: Wolters Kluwer 2019. [*Smart Contracts: a chain of trust reaching into the physical world*]

Dutch Blockchain Coalition (n.d.), *Smart contracts als specifieke toepassing van de blockchaintechnologie.* [*Smart contracts as a specific application of blockchain technology.*]

Lyons, T., Courcelas, L. and Timsit, K. Report (2018), *Blockchain Union Observatory & Forum, Blockchain and the GDPR.*

Lyons, T., Courcelas, L. and Timsit, K. Report (2019), *Blockchain Union Observatory & Forum, Legal and Regulatory Framework of Blockchains and Smart Contracts.*

Nannings, M.A.R., (2018), *Regulering van Initial Coin Offerings: een raamwerk voor regulering door de kwalificatie van tokens als effect*: 34, Weert: Celsus juridische uitgeverij 2018. [*Regulation of Initial Coin Offerings: a framework for regulation through the qualification of tokens as an effect*]

NOS Nieuws (2020), *Cryptobedrijf vertrekt door nieuwe regels: 'Mogelijk volgen er meer'*. [*Crypto company departs with new rules: "More may follow"*.]

Parliamentary Documents II 2018-2019, 32013, No 200-201.

Rank, W.A.K. (2015), *Bitcoins: civielrechtelijke en toezichtrechtelijke aspecten*, Deventer: Wolters Kluwer 2015. [*Bitcoins: civil and supervisory aspects*]

Schellekes, M., Tjong Tjin Tai, E., Kaufmann, W., Schemkes, F. and Leenes, R (2019), Tilburg University, *Blockchain en het recht. Een verkenning van de reguleringsbehoefte*, Den Haag: Ministerie van Veiligheid en Justitie. [*Blockchain and the law. An exploration of the regulatory need*]

Schuringa, H., *Enkele civielrechtelijke aspecten van blockchain*, Tijdschrift voor Computerrecht 2017/254, afl. 6: 249-291, Deventer: Wolters Kluwer. [*Some civil law aspects of blockchain*]

Szabo, N. (1997), *The Idea of Smart Contracts*, at http://szabo.best.vwh.net/smart_contracts_idea.html (consulted on 2 March 2020).

Veuger, J. (2019), *Libra and Anxiety Rhetoric: fear to be Eaten*. Res Dev Material Sci. 12(2).RDMS.000782.2019. DOI: 10.31031/RDMS.2019.12.000782.

Veuger, J. (2020), *Blockchain Convergentie*: 43. [*Blockchain Convergence*]

Zhou, Y. et al. (2018), Erays: Reverse Engineering Ethereum's Opaque Smart Contracts, *27th USENIX Security Symposium*: 1383.