EJLT European Journal of Law and Technology

Regulating Unfair Commercial Practices in a Smart Contract Context

Jasper Verstappen*

Abstract

Emerging technologies can have an impact on legal frameworks that protect consumers. This article investigates the impact of smart contract technology on the European rules regarding unfair commercial practices. It analyses the manner in which legislatures can respond to such new technologies and the impact these technologies can have on the principles of functional equivalency and technological neutrality that underpin legislative efforts. This article suggests that the potential effects of smart contract technology is such that their distinct nature must be taken into account when devising a legislative strategy aimed at modernising the law in order to ensure that the interests of consumers remain protected. It provides recommendations with regard to the manner in which the law can be designed in light of this goal and ensure that, firstly, the law is created in such a way that it can operate more consistently with governance through software and code whilst at the same time ensuring that legal enforcement is admissible in an environment governed by this technology.

Keywords: smart contracts, blockchain, unfair commercial practices, functional equivalency, technological neutrality.

---

* Jasper Verstappen (j.verstappen@rug.nl) is an assistant professor at the University of Groningen. The author wishes to thank the two anonymous referees for their insightful comments and Tim van Zuijlen for his feedback on an early draft. Any errors or omissions that remain are the responsibility of the author.

1. Introduction

In the 2020 consumer policy strategy 'The New Consumer Agenda', the European Commission acknowledges the fast pace of technological progress and recognises that, in order to protect consumer rights, additional action is needed.[1] This new policy document was released after the Modernisation Directive, in which the European legislature recognised the need to take rapid technological developments into account and update existing rules in order to cover new technologies.[2] Blockchain and smart contract technology are such new and emerging technologies that might have an impact on the operation of the European consumer *acquis* in practice. The European Law Institute (ELI) has recently published a report on the impact of this technology on the European consumer *acquis*, which follows an approach that is rooted in both functional equivalency and the doctrine technological neutrality.[3]

The scope of this article is limited to the regulation of unfair commercial practices, an area that the ELI report touches upon indirectly, and an area in which the impact of smart contracts might be severe.[4] The article explores how the European legislature can respond to the effects of this technology as far as it concerns the law on unfair commercial practices. It outlines the unique nature of the technology, analyses the law in question, and answers one central question: how can the European legislature respond to the unique nature of this technology in future revisions of the law on unfair commercial practices? The goal is to provide insights into the interactions between the legislative strategy and the technology it aims to regulate, and to

---

[1] EU Commission, 'New Consumer Agenda: Strengthening consumer resilience for sustainable recovery' (Communication) COM/2020/696 final, 10.

[2] Recitals 25 and 29 to Directive 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules ('Modernisation Directive').

[3] Report of the European Law Institute, ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection (2023), <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_Blockchain_Technology__Smart_Contracts_and_Consumer_Protection.pdf> (last accessed on 1 July 2024) (hereinafter 'ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection'); the ELI was founded in 2011 as an independent non-profit organisation: it drafts legislative proposals, model laws, model rules and statements of principles, checklists, and position papers. See: Reinhard Zimmermann, 'Challenges for the European Law Institute' (2012) 16(1) *Edinburgh Law Review* 5; European Law Institute (ELI), Manifesto (2011), <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Documents/Manifesto.pdf> (last accessed on 1 July 2024); European Law Institute, Revised ELI Project Guidelines of 13 December 2022, <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Documents/Revised_ELI_Project_Guidelines.pdf> (last accessed on 1 July 2024).

[4] See Lucas Forbes, 'Consumer Protection in the Face of Smart Contracts' (2022) 34 *Loyola Consumer Law Review* 45, 66–70.

present perspectives on the way unfair commercial practices could be regulated in a smart contract context.

Four steps are taken to answers this question. First, the technology will be outlined, illustrating its unique nature. Secondly, the principle of functional equivalency and technological neutrality will be touched upon by elaborating on the ELI's Principles on Blockchain and Smart Contract Technology. This report seeks to be both functionally equivalent to existing laws and technologically neutral, and therefore provides insights into the way that rules on consumer protection could be revised to respond to this technology. Thirdly, an overview of the existing rules on unfair commercial practices is provided. This overview is essential for the fourth and final step, which analyses how the unique nature of the technology fits into the existing legal framework.

It is concluded that tensions exist between the current legal framework on unfair commercial practices and the nature of the technology at hand. This article suggests that if the European legislature deems it necessary to revise the European rules on unfair commercial practices to account for the effects of smart contracts, the unique nature of this technology should be considered in such a revision. By doing so, an approach is suggested, for this very particular context, that diverges from the principle of technological neutrality.

2. Technology

Technological concepts such as smart contracts cannot be viewed in isolation. They are the result of a series of technological developments that must be viewed in their technical context and in relation to each other. The technology in question, as will become clear in subsequent sections, might create significant consequences for the functioning and effectiveness of the law in practice. Therefore, it is necessary to devote some attention to the technology that underpins smart contracts. Rather than elaborating on the technology itself or the developments that would eventually culminate in the technical concepts of smart contracts, this article identifies five 'key aspects'. These five key aspects are elements by which the technology must be differentiated from typical solutions. In other words, the key aspects describe how smart contracts, as technical concepts, are distinct from software, legal agreements, or other typical instruments they might support or supplant.

Those five key aspects are: immutability; transparency; pseudonymity; automatic execution; and automatic execution. The first three of these are a result of the blockchain-platform upon which smart contracts exist; the latter two are a result of

the nature of smart contracts themselves. The following sections provide an overview of these five key aspects.[5]

2.1 Blockchains

It is first necessary to establish what a blockchain is. For the purposes of this article, a blockchain will be defined as 'a collection of accounts, a ledger, supported by a system of governance, with a data structure consisting of back-linked lists of blocks of transactions in which the network collectively rather, rather than centrally, maintains the data'.[6] This system can be used as a foundation for platforms that enable participants to transact. Such blockchain platforms distinguish themselves from 'typical platforms' (ie platforms that rely on a centralised data structure) by way of three key aspects: immutability; transparency; and pseudonymity.

2.1.1 Key Aspect I – Immutability

The first key aspect is that the state of the ledger, in principle, cannot be altered by a single party or a group of parties. This immutability is guaranteed on both a transaction level and a recordation level. The former of these is a direct result of the public-key cryptography which permeates both the system of governance and the data structure. Transaction level immutability describes the fact that public-key cryptography is implemented in a manner that guarantees integrity of transactions and non-repudiation amongst the parties. Effectively this creates a system in which the technology guarantees that the content of the transaction as received corresponds to the content of the transactions as sent, while also enabling the recipient to confirm the identity of the sender.[7]

Record immutability, on the other hand, is a higher-level of immutability. It describes the integrity of the database and the immutability of information amongst the parties to the database. This second variation of immutability is a result of the set of protocols that applies amongst the participants. These protocols describe the algorithms, procedures and incentives that the network enforces amongst its participants for all participants to agree on the state of the database. These protocols are known as the 'consensus mechanism'.[8] This mechanism is essential because the network lacks a

---

[5] Please note that the technological exploration in section 2 is a summary of Jasper Verstappen, *Legal Agreements on Smart Contract Platforms in European Systems of Private Law* (Springer 2023).

[6] Definition based on Andreas Antonopoulos, *Mastering Bitcoin: programming the open blockchain* (O'Reilly Publishing 2017), 166; See for governance aspects also Kevin Werbach, *The Blockchain and the New Architecture of Trust* (MIT Press 2018), 41–48.

[7] This implementation of public key can be traced back to David Chaum, 'Blind Signatures for Untraceable Payments', in David Chaum, Ronald Rivest and Alan Sharman (eds), *Advances in Cryptology Proceedings of Crypto "82* (Springer 1983); David Chaum and Hans Van Antwerpen, 'Undeniable Signatures', in Gilles Brassard (ed) *Advances in Cryptology — CRYPTO' 89 Proceedings* (Springer 1990).

[8] Andreas Antonopoulos, *Mastering Bitcoin: programming the open blockchain* (O'Reilly Publishing 2017), 181.

central party tasked with maintaining the state of the database.[9] The Bitcoin network constitutes the first successful implementation of this technology.[10] This blockchain ensures network agreement on the state of the information by using 'a distributed computation system to conduct a "global election" every ten minutes, allowing the decentralised network to arrive at consensus on the state of transaction'.[11] This particular consensus mechanism is referred to as 'proof-of-work'. Alternative consensus mechanisms have since been developed. The proof-of-stake mechanism is, for smart contract platforms, noteworthy. This system is described as a method in which 'validator computers stake [units of value] in order to participate in agreeing on which new data to accept and in what order'.[12] The exact technological foundations of these mechanisms are beyond the scope of this article. However, it is worth noting that these mechanisms aim to ensure consensus on the state of the database as follows:[13]

- checking that units of value are authentic;
- not allowing units of value to be double-spent; and
- only allowing the rightful holder to claim ownership of a unit of value.

The consensus mechanism guarantees record immutability by ensuring that the network agrees on the state of the information within the database at any point in time.

2.1.2 Key Aspect II – Transparency

Section 0 held that a blockchain is maintained by the participants collectively. This means that the database in question exists in a distributed environment. No single party is responsible for the maintenance of the state of information, but the consensus mechanism provides a system through which all parties collectively maintain the state of the information. Doing so requires the information to be

---

[9] Several key ideas enabled the technology to be implemented in this manner; these are most notably reflected in Wei Dai, *B-money* (1998), <http://www.weidai.com/bmoney.txt> (last accessed on 1 July 2024); N Szabo, *Intrapolynomial Cryptography* (1998), <https://nakamotoinstitute.org/intrapolynomial-cryptography> (last accessed on 1 July 2024); Nick Szabo, *Trusted Third Parties are Security Holes* (2001), <https://nakamotoinstitute.org/trusted-third-parties> (last accessed on 1 July 2024); Adam Back, *A Denial of Service Counter-Measure* (2002), <http://www.hashcash.org/papers/hashcash.pdf> (last accessed on 1 July 2024); Nick Szabo, *BitGold* (2005), <https://unenumerated.blogspot.com/2005/12/bit-gold.html> (last accessed on 1 July 2024).

[10] Satoshi Nakamoto, *Bitcoin: A peer-to-peer Electronic Cash System* (2008), <https://bitcoin.org/bitcoin.pdf> (last accessed on 1 July 2024).

[11] Andreas Antonopoulos, *Mastering Bitcoin: programming the open blockchain* (O'Reilly Publishing 2017), 3–4.

[12] Vitalik Buterin and Nathan Schneider, *Proof of Stake: The Making of Ethereum and the Philosophy of Blockchains* (Seven Stories Press 2022), 253.

[13] Andreas Antonopoulos, *Mastering Bitcoin: programming the open blockchain* (O'Reilly Publishing 2017), 3.

available. Participants need to be able to check the information within transactions and information about transactions to perform the obligations that the consensus mechanism imposes on them. Transparency, in other words, is inherent to the system.

2.1.3 Key Aspect III – Pseudonymity

However, transparency is not absolute. If one were to consult a block, pick out a transaction and access that transaction, information such as the sender, the recipient, the time of the transaction and the value of the transaction would be visible. Connecting that data to a natural person is impossible with just the information that is available on the platform.

In systems based on public-key cryptography, all parties hold a key-pair. The key-pair consists of a public key and a private key. (By way of analogy, with bank accounts the public key is the bank account, and the private key is the PIN.[14]) Persons operating on the platform do so by way of their public key, which is a pseudonym. Reviewing the transaction data within the blocks on the transparent database reveals only the public key of the sender and the public key of the recipient, both of which are unique. With these keys it is therefore possible to distinguish both the sender and the recipient from all other participants.

Therefore, all information required for participants to check and verify the transactions, thereby maintaining the database, is publicly available. This includes the timing of transactions, the public keys of both senders and recipients, and the values of transactions. However, the identity of the natural person making or receiving the transaction remains hidden as no information is available (unless given, either willingly or negligently) that might connect the public key to the natural person it represents. It is for this reason that the system is transparent yet pseudonymous, but not anonymous.

2.2 Smart Contracts

The previous paragraphs discussed the blockchain and the key aspects by which it must be differentiated from typical databases. If the purpose of a blockchain is simply to store information on transactions and enable a shared record of past transactions, then a distributed ledger, as described above, suffices. Bitcoin is an example of such a platform: the bitcoin blockchain records transactions and provides little to no options for additional functionality. Some blockchains, however, do provide additional functionality by including the option to program. If the blockchain allows for programming in a manner that is sufficiently flexible, it becomes possible to run software upon that blockchain. The threshold of flexibility is referred to as 'Turing completeness'. A system is Turing complete if, given enough time, it can be used to

[14] Andres Antonopoulos and Gavin Wood, *Mastering Ethereum: Building Smart Contracts and DApps* (O'Reilly Publishing 2018), 60.

solve any solvable computational problem, regardless of its complexity.[15] The Ethereum platform, unlike the Bitcoin platform, is Turing complete: the programming-features on the Ethereum platform provide sufficient flexibility to program software applications upon that blockchain. Such software applications are referred to as 'smart contracts'. The two key aspects that define smart contracts are automatic enforcement and automatic execution.

2.2.1 Ideological Foundations

Smart contracts were conceived in 1996 by Nick Szabo and presented in *Extropy*, a journal of transhumanist thought.[16] Extropianism is a libertarian variation of transhumanism with strong anarchist elements. The ideology seeks unregulated technological progress and holds that 'an anarchistic market creates free and dynamic order, while the state and its life-stealing authoritarianism is entropic'.[17] Such principles and ideas were popular amongst the crypto-community that drove the developments that eventually culminated in tangible, functioning smart contracts. This community, also referred to as 'crypto-anarchists' or 'cypherpunks', sought to employ the technology in the development of instruments that would allow for social and economic conduct outside the reach of government.[18] As a result of this, these principles and ideas form the ideological foundations of the technology. According to Szabo, smart contracts can improve the contracting process in four ways:[19]

- they allow the parties to observe each other's performance;
- they allow the parties and arbiters to verify whether an obligation has been met or breached;
- they give parties control over the contents of the contracts and the performance, and; and
- they minimise the need for enforcement.

Szabo, a computer scientist and lawyer, presents smart contracts as if they are legal concepts. This might be explained by the nature of *Extropy*, which published his ideas – after all, this journal takes a social, rather than technological, perspective. The term 'smart contract' is rather unfortunate as it tends to evoke associations with the legal agreement. However, this article views smart contracts as technical concepts that might, under some circumstances, have applications in a legal context and could

---

[15] Ibid, 8.
[16] Nick Szabo, 'Smart Contracts: Building Blocks for Digital Free Markets' (1996) 8 *Extropy: Journal of Transhumanist Thought* 50.
[17] Janine Thweatt-Bates, *Cyborg selves* (Ashgate 2012), 50–51; Nick Bostrom, 'A History of Transhumanist Thought' (2005) 14 *Journal of Evolution and Technology* 11; James Hughes, *Citizen Cyborg: why democratic societies must respond to the redesigned human of the future* (Westview Press 2004), 164–166.
[18] See also Patrick Anderson, *Cypherpunk Ethics: Radical Ethics for the Digital Age* (Routledge 2022), 24–72.
[19] Nick Szabo, 'Smart Contracts: Building Blocks for Digital Free Markets' (1996) 8 *Extropy: Journal of Transhumanist Thought* 50.

potentially have legal relevance. These applications and legal considerations, as far as they concern the Unfair Commercial Practices Directive, will be explored in section 0 below.

2.2.2 Key Aspects IV and V – Automatic Execution and Automatic Enforcement

For years after Szabo's 1996 *Extropy* article, the idea of smart contracts remained purely theoretical. It was only in 2015, with the launch of the Ethereum platform, that the idea was successfully implemented.[20] In order to do so, Ethereum introduced the 'contract account'. These must be distinguished from 'externally owned accounts' (EOAs), which initiate and execute transactions through input provided by an individual. Contract accounts contain a set of code that defines when, and under what conditions, a certain consequence is given effect. Such consequences might take the form of a request to another contract account or to an EOA. After being uploaded to the platform, the contract requires no human input, operating automatically on the basis of the rules contained within its code, using a piece of software that runs on the Ethereum platform. The design of a contract account requires the *ex ante* stipulation of all those rules.[21] In other words, a person who designs a smart contract on the Ethereum platform creates a contract account, which requires that all relevant conditions and consequences are prescribed in the contract code. Since the programming language is Turing complete, there are no limitations on what can be programmed on the platform.[22]

The transparent nature of the platform enables the contract to observe the state of the information on the network, meaning it can determine when the conditions contained within its code are fulfilled. Once the conditions are fulfilled, the contract will execute the predefined consequence as stipulated in its code. As the contract account is controlled by the code contained within it, rather than through input that might be provided by an individual, the execution of the contract happens independently of individuals. Hence, smart contracts introduce automatic execution.

Enforcement, just like execution, happens automatically and independently of individuals. Moreover, because smart contracts exist on the database and, through their code, can interact directly with the information stored on that database, they can effectuate the conditions stipulated in their code directly on the database. This means that, as far as the patrimony of the parties exists on the database, the smart contract can interact directly and immediately with that patrimony. Since no third

---

[20] Vitalik Buterin, *Ethereum Whitepaper – A Next Generation Smart Contract & Decentralised Application Platform*, <https://ethereum.org/en/whitepaper/> (last accessed on 1 July 2024); Gavin Wood, *Ethereum: A Secure Decentralised Generalised Transaction Ledger*, <https://ethereum.github.io/yellowpaper/paper.pdf> (last accessed on 1 July 2024).
[21] Andreas Antonopoulos and GJ Wood, *Mastering Ethereum: Building Smart Contracts and DApps* (O'Reilly Publishing 2018), 27–29.
[22] Vitalik Buterin, *Ethereum Whitepaper – A Next Generation Smart Contract & Decentralised Application Platform*, <https://ethereum.org/en/whitepaper/> (last accessed on 1 July 2024), p 7.

party is necessary to effectuate the consequences, the execution of the predefined consequences happens automatically. Hence, smart contracts introduce automatic enforcement.

3. Regulating Technology

Regulating the effects and the impact of this technology presents a challenge due to its unique technological characteristics and the underlying ideological foundations. These challenges include, for example, executing and enforcing legal remedies in an immutable environment, dealing with divergences between the off-chain and on-chain state of affairs, and giving effect to rules of consumer protection in an immutable and pseudonymous context. The ELI report on blockchain and smart contract technology provides indications on how to overcome these challenges. It is built on the belief that regulation and legal certainty are drivers to innovation, meaning that both market and society at large benefit from a regulatory intervention. Moreover, it represents an effort that adheres to the core regulatory doctrine of technological neutrality. This section will provide an overview of the ELI's principles on blockchain, with special attention on consumer protection, and outline the role that the doctrine of technological neutrality plays in these principles.

3.1 Functional Equivalency and Technological Neutrality

The ELI report on blockchain technology and smart contracts has resulted in a comprehensive set of principles. The reason this project has opted for principles rather than a legislative proposal, model laws or model rules lies in the subject matter with which these principles are concerned. The drafters note that, whilst the technology is widely applied, legal doctrines are not yet sufficiently developed to deal with these novel technical concepts.[23] This creates uncertainty for all parties involved. Adopting principles allows the building of a framework for coordinated solutions among EU Member States.[24] The principles seek to support legislators in drafting sets of specific rules that are more appropriate to contracts in this field whenever a derogation from traditional contract law is fitting. Moreover, they aim to help judges in their role as interpreters of the resulting legislation.[25]

The principles are divided into a general part and a section on consumer protection. The first contains the principles that apply more generally, concerning, for example, the different types of smart contracts, private international law, the legal nature of blockchain transactions and the effectiveness of on-chain declarations of will. The latter is limited to matters of consumer protection alone. Having a separate section on consumer protection is justified by the fact that the technology can:

---

[23] ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection, 10.
[24] Ibid, 11.
[25] European Law Institute – Blockchain Technology and Smart Contracts, Aim, <https://www.europeanlawinstitute.eu/projects-publications/current-projects/current-projects/blockchains/> (last accessed on 1 July 2024).

- risk amplifying an unequal bargaining position, making it difficult to understand the legal nature of a transaction;
- obscure the conditions under which a transaction is made; and
- confront weaker parties with situations in which it is challenging or impossible to rely on instruments, such as those provided by the Unfair Commercial Practices Directive, designed to correct for the unequal bargaining position they find themselves in.

3.1.1 General

The principles recognise that smart contracts are, first and foremost, technical concepts. This is reflected by the second principle, which holds that a smart contract falls into one of four categories:[26]

1. Mere code; there is no legal agreement, and any transaction initiated in this category is a mere transfer of data.
2. A tool used to execute legal agreement.[27]
3. A legally binding declaration of will, such as an offer or acceptance or constitute the legal agreement itself.[28]
4. Merged with the legal agreement and therefore exists simultaneously both on- and off-chain.[29]

This taxonomy of smart contracts might be viewed in parallel with the UK Law Commission's classification on smart contracts, which recognises three categories of what it refers to as, 'smart legal contracts'.[30] First, the 'natural language contract with automated performance' in which some or all the obligations are performed automatically by the code. Second, the 'hybrid contract', in which some of the contractual obligations are defined in natural language and some by the computer program. Both the 'natural language contract with automated performance' and the

[26] ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection, 22; see also Jasper Verstappen, *Legal Agreements on Smart Contract Platforms in European Systems of Private Law* (Springer 2023), 172−177.
[27] For more on this, see Eric Tjong Tjin Tai, 'Smart Contracts as Execution Instead of Expression' in Jason Allen and Peter Hunn (eds), *Smart Legal Contracts: computable law and theory in practice* (Oxford University Press 2022).
[28] For more on this, see Mateja Durovic and André Janssen, 'The Formation of Blockchain-Based Smart Contracts in the Light of Contract Law' in Larry DiMatteo, Michel Cannarsa and Cristina Poncibò (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2019).
[29] For more on this, see Ian Grigg, 'Why the Ricardian Contract Came About: A Retrospective Dialogue with Lawyers' in Jason Allen and Peter Hunn (eds), *Smart Legal Contracts: computable law and theory in practice* (Oxford University Press 2022).
[30] UK Law Commission, Smart Legal Contract – Advice to Government, <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf> (last accessed on 1 July 2024), vii: 'A legally binding contract in which some or all of the contractual terms are defined in and/or performed automatically by a computer program'.

'hybrid contract', depending on the facts and circumstances of the case, encompasses what the ELI considers to be a category-2 or ELI category-3 smart contracts. Third, a contract in which all the contractual terms are defined in, and performed automatically by, the code. Depending on the facts and circumstances of the case, this seems to correspond, in my understanding, to ELI' category-3 or category-4 smart contracts.[31]

Both the UK Law Commission and the ELI offer a comprehensive categorisation of smart contracts that can encompass the various practical implementations of the technology. The ELI's categorisation is notably oriented towards recognising smart contracts primarily as technical concepts, rather than legal ones. This technical focus enables a better alignment with practical implementations and equips users of the technology with tools to pre-determine the category to which their implementation belongs. This, from the perspective of legal certainty, is an advantage.

3.1.2 Consumer Law

The final section of the report is dedicated to consumer law and the impact of the technology thereon. Initially, matters on consumer law were not explicitly within in the scope of this project, and the topic was only included after the European Commission expressed an interest in the project and voiced concerns regarding the use of the technology in relation to the consumer *acquis*.[32] During a webinar it was explained that the scope of the project was broadened after a request by the Commission to include the most challenging issues of consumer protection.[33]

The twelfth principle clarifies the goals of the sections on consumer protection and is fundamental to the approach advocated for by the ELI. It holds that weaker parties should enjoy a level of protection in an on-chain environment that is at least equal to the level of protection those weaker parties would have enjoyed in an off-chain environment. Moreover, the doctrines of technological neutrality and functional equivalency are made explicit here. The explanatory notes clarify that a solution, according to the report, ought to be technologically neutral and should achieve functional equivalency because of technology neutral law.[34]

The subsequent thirteenth principle builds on these notions by concretising the doctrine of functional equivalency in the context of relations between a consumer and a business in an on-chain environment. It holds that consumer protection cannot be overridden using blockchain technology. Moreover, protection of consumers in a

---

[31] UK Law Commission, Smart Legal Contract – Advice to Government, <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf> (last accessed on 1 July 2024), 22–23.

[32] Webinar on the ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection (1 November 2022), <https://www.youtube.com/watch?v=06X04Nqy7Gw&ab> (last accessed on 1 July 2024).

[33] Ibid.

[34] ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection, 33.

blockchain-based smart contract environment must be at least equal to consumer protection when no such technology would have been used. Hence, the use of the technology cannot deprive consumers of any rights they might have had if the technology had not been used. Additionally, the key aspects that were discussed in section 0 above − most notably immutability, automatic execution and automatic enforcement − cannot be used to deprive consumers of the rights they could have exercised under the consumer *acquis* if the technology in question was not employed. Lastly, the principle places the responsibility for ensuring consumer protection firmly with the professional party. It holds that businesses that use smart contract technology must consider the rights of consumers and ensure that their implementation of the smart contracting technology is such that the rights can be effectuated.[35]

These core sections explain both the goal and the method of the principles. The goal is functional equivalency: it is at the very core of the sections on consumer protection. The principles state that a legal solution that is binding under existing law should be binding when new technology is used. Then, the method to reach the goal of functional equivalency is the doctrine of technological neutrality: the law should provide for solutions that are binding regardless of the technology that is used by providing solutions that apply to and regulate relationships irrespective of the technology used.

The doctrines of functional equivalency and technological neutrality are therefore the foundation of the section on consumer protection. From a theoretical point of view, such a foundation is appropriate as it aligns with the character of the European consumer *acquis*.[36] However, from a practical perspective there might be challenges. In the context of smart contracts, in relation to unfair commercial practices, the doctrine of technological neutrality might not be the most effective method to reach the goal of functional equivalency. Instead, the extent to which the doctrine of technological neutrality is allowed to function as intended by the other principles outlined in the report is dependent on the mechanisms contained within the specific legal instruments that constitute the rules on unfair commercial practices. More specifically: the extent to which mechanisms contained within the Unfair Commercial Practices Directive can be reconciled with the key aspects that define the technology determine whether the doctrine of technological neutrality as a guiding principle is feasible. Within that Directive exist three mechanisms: those dealing with misleading actions and omissions; those dealing with aggressive practices; and the blacklist. By analysing how these mechanisms interact with the key aspects described in section 0, it is determined to what extent the mechanisms in the Unfair Commercial Practices Directive allow for functional equivalency. Consequently, a prediction can be made as

[35] Ibid, 40.

[36] Geraint Howells, 'European Consumer Law' in Catherine Barnard and Steve Peers (eds), *European Union Law* (Oxford University Press 2022), 728−729; Vanessa Mak and Evelyn Terryn, 'Circular Economy and Consumer Protection: The Consumer as a Citizen and the Limits of Empowerment Through Consumer Law' (2020) 43 *Journal of Consumer Policy* 227.

to whether the Unfair Commercial Practices Directive is able to accommodate smart contracts.

4. Unfair Commercial Practices Directive

The Directive provides a system of maximum harmonisation that aims to protect the economic interests of consumers in business-to-consumer (B2C) relations insofar as commercial practices of the businesses are concerned.[37] The Directive, whilst only being concerned with practices by a professional party in relation to consumers, is characterised by its broad scope. This is a result of the broad interpretation of the central terms within it: consider, for example, the notion of 'commercial practices', including 'misleading acts', 'omissions' and 'aggressive commercial practices; the concept of 'unfairness'; and the concept of 'trader'.[38]

The instruments central to the Unfair Commercial Practices Directive have been described as a three-tiered mechanism based on which it can be determined whether a commercial practice is prohibited. First, it must be determined that the commercial practice in question falls under Article 5(5) and Annex I of the Unfair Commercial Practices Directive. The Annex contains a list of those commercial practices which are by their very inclusion considered to be unfair. Secondly, it should be assessed whether the commercial practice in question might fall within one of the more abstract 'specific general clauses' which prohibit misleading acts, misleading omissions and aggressive commercial practices. Finally, the commercial practice in question should be assessed in light of the general unfairness clauses, which provide the most abstract and general mechanism on the basis of which unfairness of a commercial practice might be established.[39]

This article will apply the three-tiered structure to assess whether the doctrine of technological neutrality, as advocated for by the ELI's Principles, is a feasible method to achieve functional equivalency. First, sections 0–0 will provide a bird's-eye view of the instruments that make up the three-tiered structure. In doing so, the aim is not to be exhaustive. This examination will focus exclusively on the instruments within the Unfair Commercial Practices Directive, exploring them only insofar as is necessary

---

[37] See recitals 8, 14 and 15 of Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (hereinafter 'Unfair Commercial Practices Directive').

[38] C-59/12 *BKK Mobil Oil Körperschaft des öffentlichen Rechts v Zentrale zur Bekämpfung unlauteren Wettbewerbs eV* [2013] ECLI:EU:C:2013:634; C-388/13 *Nemzeti Fogyasztóvédelmi Hatóság v UPC Magyarország kft* [2015] ECLI:EU:C:2015:225; see also Héléne Aubry, 'Pratiques Commerciales Interdites' in Dominique Fenouillet (ed), *Droit de la consommation: droit interne et Européen* (Dalloz 2020), 239.

[39] Mateja Durovic, *European Law on Unfair Commercial Practices and Contract Law* (Bloomsbury 2016), 68.

to attain a basic understanding of their functioning. This is necessary for section 5, in which the impact of the technology, and a potential legislative response, will be explored.

4.1 Blacklist

The first tier in the three-tiered structure describes the blacklist. Annexed to the Unfair Commercial Practices Directive, the blacklist provides commercial practices that, by their very inclusion, are considered unfair. It follows from Article 5 of the Unfair Commercial Practices Directive that such practices are prohibited. The Annex showcases the Directive's maximum harmonisation across all Member States.[40] The blacklist was included in order to provide greater legal certainty: first, it enables traders, professionals and customers to identify prohibited practices more easily; secondly, it allows national enforcers to sanction such practices without having to apply a case-by-case test.[41] This list, as stipulated in Article 5(5) of the Unfair Commercial Practices Directive, can only be modified by amending the Directive. Most recently, on 27 November 2019, this was done through the Modernisation Directive. Two observations marked the start of this modernisation. First, it identified European rules contained in the consumer *acquis* that needed to be adapted to new technologies, including in particular the technologies used in the context of internet sales. Secondly, it identified which sanctions needed to be strengthened to provide more effective protection in this online context.[42] Article 13(7) of the Modernisation Directive, the transposition period of which lapsed in November 2021, included four new commercial practices in the blacklist.[43]

4.2 Misleading Acts, Misleading Omissions and Aggressive Practices

The second tier in the three-tiered structure prohibits misleading actions, misleading omissions and aggressive practices.[44] The first of these includes giving false, untruthful or deceptive information, creating confusion with competitors' products, trademarks, names and distinguished marks, and non-compliance with firm and verifiable commitments contained in a code of conduct to which the traders indicated they would be bound.[45] Such practices are prohibited by Article 6 of the Unfair Commercial Practices Directive. Secondly, it follows from Article 7 of the Directive

---

[40] Willem van Boom, 'Unfair Commercial Practices' in Christian Twigg-Flesner (ed), *Research Handbook on EU Consumer and Contract Law* (Edward Elgar 2016), 397.
[41] EU Commission Notice OJ C 526, 29.12.2021, p. 61.
[42] See recitals 25 and 29 to the Modernisation Directive; Héléne Aubry, 'Pratiques Commerciales Interdites' in Dominique Fenouillet (ed), *Droit de la consommation: droit interne et Européen* (Dalloz 2020), 240.
[43] Bram Duivenvoorde, 'The Upcoming Changes in the Unfair Commercial Practices Directive: A Better Dea for Consumers?' (2019) 8(6) *Journal of European Consumer and Market Law* 219.
[44] See Articles 5−7 Unfair Commercial Practices Directive.
[45] Willem van Boom, 'Unfair Commercial Practices' in Christian Twigg-Flesner (ed), *Research Handbook on EU Consumer and Contract Law* (Edward Elgar 2016), 393; see also Hugh Collins, 'Harmonisation by Example: European Laws against Unfair Commercial Practices' (2010) 73(1) *Modern Law Review* 89, 101−102.

that an omission is misleading if it omits information that the average consumer needs, in the relevant context, to make an informed decision.[46] The same holds true for the trader that discloses such information in an unclear, unintelligible, ambiguous or untimely manner.[47] It should be noted that such omissions are only prohibited if they caused or are likely to have caused the average consumer to take a decision that they would not otherwise have taken.[48] Thirdly, there are the aggressive practices which are defined by Article 9 Unfair Commercial Practices Directive as 'harassment, coercion, including the use of physical force, or undue influence that significantly impairs or is likely to significantly impair the average consumer's freedom of choice with regard to the product and thereby causes him or is likely to cause him to take a transactional decision that he would not have taken otherwise'.[49]

4.3 General Unfairness Clause

The final tier of the three-tiered system that forms the core of the European regime on unfair commercial practices can be found in Article 5 of the Unfair Commercial Practices Directive. This Article has been referred to as a 'safety net' as, once a certain practice falls in one of the preceding tiers of the three-tiered system, it is no longer necessary to test whether it meets the conditions stipulated in Article 5.[50] This Article prohibits those commercial practices that are contrary to the requirements of professional diligence and distort, or are likely to distort, the economic behaviour of the average consumer.[51] The standard of 'professional diligence' provides what has been described as 'a normative yardstick', ie it requires a standard of special skill and care which a trader may reasonably be expected to exercise towards consumers, commensurate with either an honest market practice in the trader's field or the general principle of good faith.[52] Additionally, 'material distortion' in this context is defined by the Directive as the potential of a commercial practice to appreciably

---

[46] See on the notion of 'average consumer' in Mateja Durovic, *European Law on Unfair Commercial Practices and Contract Law* (Bloomsbury 2016), 29–39.

[47] Willem van Boom, 'Unfair Commercial Practices' in Christian Twigg-Flesner (ed), *Research Handbook on EU Consumer and Contract Law* (Edward Elgar 2016), 392; Hugh Collins, 'Harmonisation by Example: European Laws against Unfair Commercial Practices' (2010) 73(1) *Modern Law Review* 89, 104−107.

[48] C-281/12 *Trente Sviluppo and Centrale Adriaticia* [2013] ECLI:EU:C:2013:859.

[49] See for more on this Fausto Caronna, 'Tackling Aggressive Commercial Practices: Court of Justice Case Law on the Unfair Commercial Practices Directive Ten Years On' (2016) 43(6) *European Law Review* 880.

[50] Willem van Boom, 'Unfair Commercial Practices' in Christian Twigg-Flesner (ed), *Research Handbook on EU Consumer and Contract Law* (Edward Elgar 2016), 391; see also Hugh Collins, 'Harmonisation by Example: European Laws against Unfair Commercial Practices' (2010) 73(1) *Modern Law Review* 89, 99; C-435/11 *CHS Tour Services GmbH v Team4 Travel GmbH* [2013] ECLI:EU:C:2013:574; C-388/13 *Nemzeti Fogyasztóvédelmi Hatóság v UPC Magyarország kft.* [2015] ECLI:EU:C:2015:225.

[51] See recitals 11 and 13 to the Unfair Commercial Practices Directive.

[52] Willem van Boom, Amandine Garde and Orkun Akseli, 'Introduction' in Willem van Boom, Amandine Garde and Orkun Akseli (eds) *The European Unfair Commercial Practices Directive* (Routledge, 2014), 2.

impair the consumer's ability to make an informed decision that causes the consumer to take a transactional decision that he would not otherwise have taken. Here the Directive applies a hypothetical standard of causality, requiring the determination of what the 'reasonably well-informed and reasonably observant and circumspect consumer', rather than the actual consumer, would have done.[53]

5. Providing Legal Protection to Consumers in a Smart Contract Context

The three tiers of the system at the heart of the Unfair Commercial Practices Directive introduce norms that are progressively open.[54] The blacklist, in comparison to the subsequent tiers, provides a relatively closed norm as it contains an exhaustive list containing detailed descriptions of commercial practices that, due to their very inclusion in that list, are prohibited. The following two tiers of the three-tiered system provide increasingly open-ended instruments. The second tier, for example, requires a person who relies on the Directive to establish that certain information was untruthful, the trader was deceptive, or that information was omitted that was required by the average consumer in order to make an informed decision and who would, in the absence of that information, make a different decision. Lastly, the general unfairness clause is the most open-ended tier. This aligns with its 'safety net' function. In addition to relying on the ambiguous concept of 'average consumer', it also presents the concepts of 'commercial diligence' and 'material distortion'.

Open norms and ambiguous concepts that require a case-by-case assessment of relevant facts and circumstances are difficult to reconcile with the technology. It is possible that specific legal standards are highly incompatible with the technology in question. Consider, for example, a legal standard that mandates an arbiter to discern relevant facts and circumstances, interpret the perception of such facts and circumstances by the involved parties, establish the intentions underlying all that has transpired, and determine what each person might have reasonably concluded from those facts and circumstances. This is exactly what the final tier of the Unfair Commercial Practices Directive requires. The technology, due to its very nature, is

---

[53] Article 2(e) Unfair Commercial Practices Directive; Willem van Boom, 'Unfair Commercial Practices' in Christian Twigg-Flesner (ed), *Research Handbook on EU Consumer and Contract Law* (Edward Elgar 2016), 391; Hugh Collins, 'Harmonisation by Example: European Laws against Unfair Commercial Practices' (2010) 73(1) *Modern Law Review* 89, 98–99; C-210/96 *Gut Springenheide GmbH and Rudolf Tusky v Oberkreisdirektor des Kreises Steinfurt – Amt für Lebensmittelüberwachung* [1998] ECLI:EU:C:1998:36; C-470/93 *Verein gegen Unwesen in Handel und Gewerbe Köln eV v Mars GmbH* [1995] ECLI:EU:C:1995:224 and C-373/90 *Criminal proceedings against X* [1992] ECLI:EU:C:1992:17; for more on this see Mateja Durovic, *European Law on Unfair Commercial Practices and Contract Law* (Bloomsbury 2016), 30–33.

[54] As concluded by Willem van Boom, 'Experiencing Unfair Commercial Practices: An Introduction' (2012) 5(4) *Erasmus Law Review* 233, 236; see also Charlotte Pavillon, *Open Normen in het Europees Consumentenrecht: de Oneerlijkheidsnorm in Vergelijkend Perspectief* (Kluwer 2011).

unsuitable for dealing with such legal standards. The reason for this is simple: machines and computers speak a different language.

5.1 Machine Language and Human Language

Szabo pointed out the difference between what he called 'wet code', ie information as interpreted by the brain, and 'dry code', ie information interpreted by machines.[55] Examples of the former include human-read media like newspapers and academic journals, whilst examples of the latter include bytecode and binary files.[56] Terms such as 'natural language' and 'formal language' are perhaps more appropriate as they reflect the nature of the languages more adequately and, with regard to natural language, provide a stronger indication of the connection between words and the things they represent, as well as the manner in which words acquire meaning.[57]

In this context it is relevant to distinguish between subjective and objective information. 'Subjective information', or 'subjective statements', refers to information that is not factual in nature. Such information might reflect an opinion, a personal view, an experience or a belief. Objective information is the inverse to subjective information: it relates to facts and is devoid of opinion, views, experience or beliefs. The difference between wet code and dry code lies in the fact that dry code, relative to wet code, is more suitable in dealing with objective information: it can do so more quickly, cheaply and accurately. Wet code, on the other hand, is more suitable for dealing with subjective information: it can assess the relative importance of different facts and circumstances, and incorporate the subtle differences of perception that are pivotal to such assessments.

The instruments of the Unfair Commercial Practices Directive illustrate that objectivity and subjectivity are not alternatives, but exist on opposite ends of a spectrum. Tier one, the blacklist, is relatively objective in nature. It contains a well-defined and closed list of commercial practices. The first entry of the blacklist, for example, stipulates that 'claiming to be a signatory to a code of conduct when the trader is not' is an unfair commercial practice. This is an example of an instrument relying exclusively on objective information. Establishing, in a concrete situation, whether the conduct of a trader on a smart contract platform meets the standard stipulated in the first entry of the blacklist can be automated through software running on that platform. A computer program, or a smart contract, can ascertain that a trader claims to be a signatory to a code of conduct and, subsequently, consult the registry of signatories to that code of conduct. By doing so, the smart contract can determine whether the standard imposed by the Directive is met. Such a legal instrument aligns well with the nature of the technology at hand. The blacklist is

---

[55] Nick Szabo, 'Wet code and dry' (2006) <http://unenumerated.blogspot.com/2006/11/wet-code-and-dry.html> (last accessed on 1 July 2024).
[56] Ibid.
[57] Jason Allen, '"Smart Contracts" and the Interaction of Natural and Formal Language' in Jason Allen and Peter Hunn (eds), *Smart Legal Contracts: computable law and theory in practice* (Oxford University Press, 2022), 36 et seq.

therefore wet code that is well-suited to be converted into dry code. The second and the third tier of the Directive include increasingly subjective elements. As such, they are less suited to be converted into dry code. To determine, for example, whether the standard created by the general unfairness clause of the Unfair Commercial Practices Directive is met, a smart contract would have to determine whether a certain practice is contrary to professional diligence and is likely to distort the economic behaviour of the average consumer. Such information, contrary to the determination of whether a particular trader is a signatory to a code of conduct, is subjective in nature: it depends on experiences, a weighing of assessments and interpretations, and the concretisation, in consideration of particular circumstances, of open standards. Software is unable to do this with the same effectiveness as humans. As the Directive's three-tiered system becomes more subjective, the technology in focus here becomes less compatible with the legal instruments contained therein.

5.2 Technological Neutrality and Legislating Smart Contract Technology

The observation that some legal instruments might be incompatible with blockchain and smart contract technology does not render the two fundamentally irreconcilable. This article does not advocate for a radical understanding of 'code is law' ie, the idea that technology can (or should) supplant the law, or take over the social function of law.[58] Quite the contrary; in order to legislate blockchain and smart contract technology, the nature of the technology must be taken into account. In other words, to legislate in this area, the common legislative instruments must be reassessed and due consideration must be given to the legislative strategy that is chosen. This technology might force the legislature to be pragmatic and creative. However, doing so might create tension between the doctrine of technological neutrality as a method to achieve functional equivalency, and the legal intervention that the technology requires in light of the goal of providing adequate protection to consumers.

The doctrine of technological neutrality asserts that regulations must be neutral regarding the technology that is subject to the regulation.[59] Four distinct but interlinked rationales are at the core of the doctrine of technological neutrality: non-discrimination; sustainability; efficiency; and consumer certainty.[60] This doctrine is central in European Union law, especially within the realm of consumer law, as far as

---

[58] As Lawrence Lessig, *Code: And Other Laws of Cyberspace, Version 2.0* (Basic Books 2006) is often represented; see in this context also Marisaria Maugeri, 'Smart Contracts, Consumer Protection, and Competing European Narratives of Private Law' (2022) 23(6) *German Law Journal* 900.

[59] Commission, 'Towards a new framework for Electronic Communications infrastructure and associated services' (Communication) COM(00) 539 final.

[60] Ilse M van der Haar, 'The principle of technological Neutrality: Connecting EC network and content regulation' (doctoral thesis, Tilburg University 2008), < https://research.tilburguniversity.edu/files/1063437/3240352.pdf> (last accessed on 1 July 2024), 96–102.

the regulation of technology is concerned.[61] It holds that, rather than regulating the technology itself, the effects and the function of the technology must be regulated.[62] Focusing regulatory efforts on the manner in which technology is used and the effects it creates for society at large, rather than focusing on the technology itself, ensures that the legislative intervention is flexible and future-proof. This creates a legislative framework that pre-empts continued technological evolution and provides a stable framework for both business and consumers.[63] Such an approach reflects the previously mentioned rationales of sustainability and consumer certainty underlying the doctrine of technological neutrality.

The ELI Principles follow an approach that is aimed at creating a functionally equivalent legal framework through technological neutrality.[64] This article argues that the nature of blockchain and smart contract technology is such that some legal instruments in the current legal framework lose some of their effectiveness in a blockchain-based smart contract environment. This suggests a tension between the approach taken by the European Law Institute and the inherent nature of the technology, at least as far as the regulation of unfair commercial practices is concerned. It follows from the twelfth and thirteenth principle in the ELI Report that consumer protection on a blockchain-based smart contract platform should be equal to or greater than the protection available in a non-blockchain context.

This objective, combined with the distinct characteristics of the technology at hand, causes a tension between functional equivalency on the one hand, and the doctrine of technological neutrality on the other hand. This tension could be resolved by taking the unique nature of this technology into account in future revisions of the rules on consumer protection in general, and unfair commercial practices in particular. Instead, the nature and unique characteristics of the technology at hand should be considered. While acknowledging the importance of technology-neutral considerations, an approach that specifically addresses the distinctive aspects of this technology is more likely to be effective in regulating this specific technology. This

---

[61] See for example Leigh Hancher and Pierre Larouche, 'The Coming of Age of EU Regulation of Network Industries and Services of General Economic Interest' in Paul Craig and Grainne De Burca (eds), *The Evolution of EU Law* (2nd edn, Oxford University Press 2011) and G Howells, 'Protecting Consumer Protection Values in the Fourth Industrial Revolution' (2020) 43 *Journal of Consumer Policy* 145.

[62] Bert-Jaap Koops, 'Should ICT Regulation Be Technology-Neutral?' in Bert-Jaap Koops and others, *Starting Points for ICT Regulation*, vol 9 (TMC Asser Press 2006) 6; Brad Greenberg, 'Rethinking technological neutrality' (2015) 100 *Minnesota Law Review* 1495, 1512.

[63] Ilse M van der Haar, 'The principle of technological Neutrality: Connecting EC network and content regulation' (doctoral thesis, Tilburg University 2008), < https://research.tilburguniversity.edu/files/1063437/3240352.pdf> (last accessed on 1 July 2024), 98; Jakub Harasta, 'Trust by Discrimination: Technology specific Regulation & Explainable AI' (International Conference on Legal Knowledge and Information Systems (JURIX 2018), Groningen, December 2018), <https://ceur-ws.org/Vol-2381/xaila2018_paper_3.pdf> (last accessed on 1 July 2024).

[64] ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection, 9 and 33.

approach aims to ensure that consumers receive a level of protection within a blockchain environment that is at least equivalent with non-blockchain environments.

5.3 An Alternative Approach: on Code-like Law and Law-like Code

Such an approach, guided by the distinct nature of the technology, can be distilled from the framework proposed by Werbach, which is composed of two interactive strategies: make law more code-like; and code more law-like. The goal of the framework is to reconcile legal and cryptographic enforcement.[65] This framework takes the specific nature of the technology at hand into account, providing guidance on the basis of which an approach could be devised for use by the European legislature in future revisions of the laws applicable to unfair commercial practices.

5.3.1 Making Law More Code-like

The idea underlying the first strategy − making the law more code-like − is that the technology in question should stimulate innovative solutions through which the law can operate more consistently with governance through software and code. When presenting his framework, Werbach gives four examples of making law more code-like: safe harbours; sandboxes; modularised contracts; and information fiduciaries. Modularised contracts are the most relevant of these for the purposes of this article. The contracting process, in the absence of any smart contracting technology, is already heavily modularised. Lawyers reuse standard clauses on, for example, damages or exonerations. An identical system might be employed for smart contracts, in which such standard clauses might be presented as components in a digital document using a mark-up language. Effectively, this would create a situation in which the legal contracting process is set up in a manner that resembles the programming process of the smart contract.[66] Such a system allows the two to more easily interact and respond to each other. Moreover, this approach can reduce the risk of software being used to facilitate prohibited unfair commercial practices on-chain. This can be done by creating standards for common legal clauses as well as common programming components. The European legislature can take charge of the creation of such modules and make their inclusion mandatory. The discussion about the code of conduct in section 5.1 is an excellent example of a legal instrument that can be transformed into a smart contract module, the incorporation of which can be mandated on a platform-level. Just as standard terms and conditions can be modularised in smart contract code, the same holds true for mandatory law: doing so guarantees that these commercial practices are barred from being exercised through the very programming.

In this scenario, the role of a lawyer may be different, but remains crucial. Lawyers play a pivotal role in defining the unfair commercial practices within the general modules that must be created by a programmer. Their tasks might include, for

---

[65] Kevin Werbach, *The Blockchain and the New Architecture of Trust* (MIT Press 2018), 204.
[66] Ibid, 206.

example, assisting clients in identifying which modules are relevant for their legal agreement or smart contract, and helping them to negotiate these agreements while tailoring the modules to suit their specific requirements. For concrete legal relations, the technology forces parties to carefully consider eventualities as retroactively adjusting the components is complicated, but not impossible. Again, this illustrates the essential role that a lawyer will play in this context. Additionally, lawyers must be involved in the development process of these smart contract modules. Their input is essential in translating the natural language of the law into formal language that is suitable to be included in a smart contract platform.

Regarding the Unfair Commercial Practices Directive specifically, the designer or operator of a smart contract platform could employ a modularisation approach to mitigate as much as possible the chances of unfair commercial practices occurring on their platform. This task might even be taken up by the legislature itself. The greater the dependence of the legal instruments contained within the Directive on subjective information and assessments, the less compatible the technology is with such legal instruments. In practice this might mean that the technology could be unsuitable for implementation in this specific context. One previous example of this relates to trust and quality marks. The designer or operator determines which trust marks or quality marks are appropriate for the type of business for which the smart contract platform is designed. Based on this determination, he can then present persons operating on that platform with a pre-programmed smart contract module that, after automatically having determined whether a particular party has a right to carry the mark in question, they can run to present the trust mark or quality mark, thereby effectively implementing the second entry to the blacklist annexed to the Unfair Commercial Practices Directive.

However, an example of an instrument that is less suitable to be implemented through the technology, for reasons that were elaborated upon previously, is the general unfairness clause which forms the third-tier of the Directive. Even in this context, the technology might be used to mitigate, albeit to a lesser extent when compared to the more objective first-tier, the occurrence of unfair commercial practices on the platform through modularised smart contracts. By thoroughly examining existing applicable case law, a designer or operator of a smart contract platform can ascertain specific actions that professional diligence might impose on traders on that platform. Such an analysis helps identify behaviours that are likely to distort the behaviour of an average consumer and what sort of acts might impact the economic behaviour of a consumer in an unacceptable manner in this specific context.

5.3.2 Making Code more Law-like

The second strategy − making code more law-like − is aimed at ensuring that legal enforcement is more admissible in a blockchain-based smart contract environment. Examples of such methods include the integration of terms of legal and smart contracts, the integration of traditional legal enforcement mechanism into smart contracts, and the integration of law-like governance processes into blockchain

platforms.[67] Traditional legal enforcement mechanisms might be integrated in smart contracts through oracles. Oracles are defined in the ELI's principles as 'services that update a blockchain using data outside that blockchain'.[68] It is, in other words, a system that transfers data from outside the blockchain in a computer-readable form into the blockchain. A simple example of a legal agreement programmed into a smart contract needing an oracle is an insurance agreement in which the premium will be paid out once a certain weather event, eg a flood, occurs. The legal agreement can be programmed fully upon the blockchain as a smart contract, but needs off-chain data (ie water levels) to determine when the predefined condition for paying the premium has been met. A water sensor functions as an oracle to introduce data that exists outside the blockchain into the blockchain.[69]

A smart contract, as was explained in section 0, is both automatically executing and automatically enforcing. An oracle effectively provides a method through which the aspect of automatic execution or automatic enforcement can be weakened. In the previously mentioned example of the insurance agreement programmed into a smart contract, the oracle functions as a condition external to the smart contract upon its enforcement. Hence, the oracle weakens the automatic enforcement of the smart contract.

An oracle can also weaken the automatic execution aspect. A scenario that exemplifies this situation arises in an escrow-style set-up where, instead of directly executing a smart contract between the intended recipient and sender, the transaction's object is initially transferred to a trusted intermediary. This trusted intermediary can be a smart contract specifically designed and audited for this purpose, or an actual person.[70] The intermediary can verify that the smart contract that effectuates the transfer itself reflects the intentions of the parties and transfer onwards to the intended recipients the objects of the transaction. If not, the oracle can reverse the transaction.[71] Such a system can even be used to implement full arbitration in a smart contract context.[72]

Oracles illustrate one method through which legal enforcement mechanisms can be introduced in a blockchain and smart contract context. This provides an avenue for

---

[67] Ibid, 212.
[68] ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection, 20.
[69] Andres Antonopoulos and Gavin Wood, *Mastering Ethereum: Building Smart Contracts and DApps* (O'Reilly Publishing 2018), 253 et seq.
[70] Conferring the role of an oracle upon a person can be done by using a multisig function; see Andres Antonopoulos and Gavin Wood, *Mastering Ethereum: Building Smart Contracts and DApps* (O'Reilly Publishing 2018), 123–124. A full technical exploration of this is, for reasons of conciseness, out of scope for this contribution.
[71] Defined by ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection, 20 as 'opposing transaction where the originally executed transaction is reversed by a subsequent, exactly opposing transaction'.
[72] Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018), 74.

programmers and legislatures wanting to incorporate the rules contained with the Unfair Commercial Practices Directive in a manner that is consistent with the principle of functional equivalence as reflected by the ELI's principles on blockchain technology and smart contracts.

6. Final Remarks

The technology in question has the potential to impact the consumer *acquis* in general, and the Unfair Commercial Practices Directive more specifically. The European Commission observed that 'the digital transformation is radically changing consumers' lives', and that 'considering the fast pace of the technological progress and its impact on the consumer experience, additional action is needed'.[73] This article has investigated smart contract technology as an emerging technology and argued that, with adequate protection as the goal of a regulatory intervention, a tension exists between functional equivalency and the doctrine of technological neutrality.

This article set out to determine how the European legislature could respond to the effects of this technology in light of that tension, as far as the rules on unfair commercial practices are concerned. In this context inspiration was drawn from the ELI report on blockchain and smart contract technology. This report takes as its starting point the existing tenets of regulatory intervention in technology law: the goal is to create a set of regulations that are functionally equivalent, and the method to do so is based on the doctrine of technological neutrality. The tension that exists between functionally equivalent regulation of the technology at hand and the doctrine of technological neutrality should prompt the European legislature to consider alternative legislative strategies in future revisions of the rules on unfair commercial practices. Such strategies should consider the unique nature of this technology. Two suggestions on how this could be achieved have been made.

First, the legislature should aim to create a legal toolbox that operates as consistently as possible with governance through software. Section 0 explored modularised contracts as an example hereof. Secondly, the legislature should ensure as far as possible that smart contract platforms are designed in way that allows legal enforcement measures to function upon that platform. This can be done by involving operators or designers of such platforms in the legislative process and by ensuring that in the design phase (*ex ante*) of the platform certain safeguards are hardcoded into the platform. By doing so, functional equivalency can be achieved by explicitly taking the nature of the technology into account. Section 0 explored oracles as an example hereof. These two interacting strategies, as proposed by Werbach, have respectively been referred to as 'making law-like code' and 'making code-like law'.

It should be noted that such an approach might result in a weakening of the key aspects that make this technology unique. The oracle-example explored earlier has a

[73] EU Commission, 'New Consumer Agenda: Strengthening consumer resilience for sustainable recovery' (Communication) COM/2020/696 final, 10.

direct impact on automatic execution and automatic enforcement. A person or business experimenting with the technology might ask a simple question: 'why implement the technology if the law requires the weakening of that unique selling points of this technology?'. This question is not a legal question. If the technology is such that it might have such an impact on consumer protection that it, considering the policy considerations underlying the relevant legal framework, goes beyond what is acceptable, then a legislative response that limits those aspects is proportionate. It is up to the legislature to strike a balance between consumer protection and innovation. Once such a balance is struck through concrete legal action, the question whether the technology is viable and should be implemented can only be answered through a cost–benefit analysis. Such an analysis is for entrepreneurs, rather than lawyers. Lawyers should be concerned with the fundamental preliminary question to this. One such preliminary question was at the heart of this article: how should the European legislature respond to the technology? One fundamental goal of consumer law is to provide adequate protection to consumers. In the context of this technology, that goal should prompt the legislature to take the nature of the technology into account.