ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection

The European Law Institute

The European Law Institute (ELI) is an independent non-profit organisation established to initiate, conduct and facilitate research, make recommendations and provide practical guidance in the field of European legal development. Building on the wealth of diverse legal traditions, its mission is the quest for better law-making in Europe and the enhancement of European legal integration. By its endeavours, ELI seeks to contribute to the formation of a more vigorous European legal community, integrating the achievements of the various legal cultures, endorsing the value of comparative knowledge, and taking a genuinely pan-European perspective. As such, its work covers all branches of the law: substantive and procedural; private and public.

ELI is committed to the principles of comprehensiveness and collaborative working, thus striving to bridge the oft-perceived gap between the different legal cultures, between public and private law, as well as between scholarship and practice. To further that commitment it seeks to involve a diverse range of personalities, reflecting the richness of the legal traditions, legal disciplines and vocational frameworks found throughout Europe. ELI is also open to the use of different methodological approaches and to canvassing insights and perspectives from as wide an audience as possible of those who share its vision.

European Law Institute
Schottenring 16/175
1010 Vienna
Austria
Tel: + 43 1 4277 22101
E-mail: secretariat@europeanlawinstitute.eu
Website: www.europeanlawinstitute.eu

Approved by the ELI Council on 5 July 2022 and by the ELI Membership on 8 September 2022.
Council Draft and final drafted published on 8 September 2022 and 16 February 2023 respectively.

ISBN: 978-3-9505192-9-7

This publication was co-funded by the European Union's Justice Programme. Acknowledgment is also due to the University of Vienna, which has generously hosted the ELI Secretariat under successive Framework Cooperation Agreements since 2011.

This project is co-funded by the European Union

Table of Contents

ACKNOWLEDGEMENTS

Project Team

Project Chair and Reporter

Sjef van Erp (Professor, The Netherlands)

Project Reporters
Martin Hanzl (Practising Lawyer, Austria)
Juliette Sénéchal (Professor, France; until January 2021)

Other Members of the Project Team

Adrien Basdevant (Practising Lawyer, France)
Raffaele Battaglini (Practising Lawyer, Italy)
Vincent Danos (Professor, France)
Primavera de Filippi (Researcher, France)
Michele Marchesi (Professor, Italy)
William McKechnie (Judge, Ireland)
Denis Philippe (Professor, Belgium)
Pascal Pichonnaz (Professor, Switzerland)
Ernst Steigenga (Practising Lawyer, The Netherlands)
Teresa Touriñán (Land Registrar, Spain)
Jos Uitdehaag (Practising Lawyer, The Netherlands)
Jasper Verstappen (Practising Lawyer, The Netherlands)
Aura Esther Vilalta Nicuesa (Professor, Spain)
Jacques Vos (Registrar, The Netherlands)
Aneta Wiewiórowska-Domagalska (Professor, Poland)
Christopher Wray (Practising Lawyer, United Kingdom)
Filippo Zatti (Professor, Italy)
Fryderyk Zoll (Professor, Poland)

Advisory Committee

Assessors

Christoph Busch (Professor, Germany)
Teresa Rodríguez de las Heras Ballell (Professor, Spain)
Pietro Sirena (Professor, Italy)

Other Members

Hans Schulte-Nölke (Professor, Germany)
Christiane Wendehorst (Professor, Austria)
Célia Zolynski (Professor, France)

Members Consultative Committee

Individuals
Despoina Anagnostopoulou (Professor, Greece)
Arvind Babajee (Corporate Jurist / Chartered Management Accountant, Mauritius)
Anurag Bana (Practising Lawyer, India)
Małgorzata Boszko (Practising Lawyer, Poland)
Daniele Busani (Practising Lawyer, Italy)
Pınar Çağlayan Aksoy (Researcher, Turkey)
Ana Cediel (Practicing Lawyer, Spain)
Claudio Cipollini (Researcher, Italy)
Moustapha Ebaid (Researcher, Palestine)
Marco Giacalone (Researcher, Italy)
Francisco Javier Jiménez Muñoz (Professor, Spain)
Marina Kasatkina (Researcher, Russia)
Antonio Legerén Molina (Professor, Spain)
Matthias Lehmann (Professor, Germany)
Francesco Longobucco (Professor, Italy)
Vadims Mantrovs (Researcher, Latvia)
Kiril Mitrov (Researcher, Macedonia/Bulgaria)
Alberto Monti (Professor, Italy)
Sophie Moreil (Lecturer, France)
Dimitrios Moustakatos (Practising Lawyer, Greece)
Elena Alina Ontanu (Professor, Romania)
Albert Ruda (Professor, Spain; Chairperson)
Leigh Sagar (Practising Lawyer, United Kingdom; Deputy Chairperson)
Roberto Sammarchi (Practising Lawyer, Italy)
María Elena Sánchez Jordan (Professor, Spain)
Vijay Kumar Singh (Researcher, india)
Alina Škiljić (Practising Lawyer, Croatia)
Dejan Ukropina (Practising Lawyer, Serbia)

Institutions
American Constitution Society (represented by Timothy Burns)
Austrian Chamber of Civil Law Notaries (represented by Stephan Matyk-d'Anjony)
Blockchain Education Network Italia (represented by Niccolò Travia)

Centre for Legal and Economic Research (represented by Maria Raquel Guimarães)
Curia of Hungary (represented by László Czibulka)
European Law Students Association (ELSA Austria, represented by Arsen Hovakimyan)
European Union of Judges in Commercial Matters (UEMC, represented by Rainer Sedelmayer)
Izmir University of Economics, Faculty of Law of (represented by Huriye Kubilaj)
'Vasile Goldis' Western University of Arad (represented by Christian Alunaru†)
University of Latvia (represented by Janis Karklins)

Observer

Hungarian Chamber of Civil Law Notaries (represented by Tamás Parti and Tamás Sajben)

ELI Project Officer

Tomasz Dudek (Senior Project Officer, Austria)

Executive Summary

The project started in 2018 following a **Use-Case Approach** (ie a descriptive and up-close exploratory examination of how a blockchain could function in a real-world context) to understand how blockchains and Smart Contracts might be used in practice. However, developments were moving so fast that sometimes, shortly after a use-case was presented, the experience gained from such a case was already surpassed by later developments.

Thus, the Reporters, and the Project Team, decided to focus more on the legal aspects of blockchains and Smart Contracts, both in a commercial and a consumer setting and to develop corresponding theories, which could ultimately result in Principles. Before theories were formulated as Principles, they were tested against known use-cases to ensure their practicability.

This helped us to understand the following:

(i) Rapid innovation**:** Distributed Ledger Technology (or DLT, including blockchain technology) is evolving daily and many use-cases are still at the proof-of-concept stage. As a result, new business models and also legal challenges constantly arise.

(ii) As to blockchain technology, four main types exist: public, alongside private blockchains, where both types can be permissionless or permissioned. In practice, many private and permissioned blockchain projects are being developed which do not attract the same amount of attention as public and permissionless projects such as Bitcoin. It is, therefore, important to keep abreast of what is happening in practice. This not only holds true for what is taking place in areas such as the securing of finance (financial technology or 'FinTech'), providing property services (property technology or 'PropTech') and other more traditional private law areas, but also for what is happening in public law, for example at European Economic Area (EEA) level in the European Blockchain Services Infrastructure (EBSI).[1] Within EBSI, one of the use-cases was 'notarisation' in the sense of 'immutable proof of authenticity/integrity of a given file'; not to be mistaken with the drawing up of authentic documents by civil law notaries.[2] In the near future these developments regarding the use of blockchain technology in public law may have a considerable impact on private law actors.

(iii) It is necessary not only to assess Smart Contracts from a legal (and technological) perspective, but also to take into account the infrastructure in which they are operating, as this usually affects Smart Contracts. The question of Smart Contracts (as well as the question of Initial Coin Offerings (ICOs), tokens, crypto-assets (particularly cryptocurrencies) or the question of dispute resolution systems on chain) is inextricably linked to an infrastructure/system and a community that make this infrastructure/system work.

(iv) Smart Contracts have the potential to automate and simplify many transactions. Due to their complex technological design and the embedding of Smart Contracts in blockchains, the use of Smart Contracts raises many legal questions, which is why such use should perhaps be better

1 <https://ec.europa.eu/digital-building-blocks/wikis/display/ebsi> accessed 16 November 2022.

2 <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/%5Barchived%5DNotarisation+User+Stories> accessed 16 November 2022.

considered holistically, ie from an integrated technology-legal perspective. This would imply that not only a private law and a public regulatory, but also a sandbox approach would have to be considered, and not just separately, but in an integrated way. Although this approach, at least to a certain degree, can already be found in recent national blockchain legislation, in this report the prime focus will be on the private law approach, to provide at least some initial clarity about the legal effectiveness of blockchain transactions and Smart Contracts.[3] This also implies that, although DLT and Smart Contracts might be used in transactions between Governments (G2G), Business and Government (B2G), and Governments and private citizens/Consumers (G2C), the ELI Principles are not intended to govern such types of transactions, which are frequently more of a public than a private law nature. Besides these legal governance approaches, a more innovative-technical approach can also be usefully aimed at testing the functioning of a blockchain and the use of Smart Contracts. This can be done in a so-called 'sandbox': a legal environment which provides freedom for testing without liability risks for developers, but also ensuring that the users of, for example, a platform are fully protected against failures which might arise.[4] An example is the European Blockchain Partnership, which is building the EBSI, creating a technological and regulatory sandbox.[5]

(v) Given the rapid technological developments and the still considerable lack of national and international regulation, as well as the rather limited existence of case law, we only propose a limited set of Principles on the legal governance of blockchains and Smart Contracts. The Principles focus on contract law. Furthermore, we are very aware of the need to draw clear distinctions between different types of users, depending on their relative understanding, knowledge and experience. More particularly, we clearly distinguish between Business to Business (B2B) and Business to Consumer (B2C) relations as a fundamental difference exists between business and consumer transactions. A further differentiation could be made regarding Government to Government (G2G), B2G and G2C relations, but such transactions frequently show more public law than private law characteristics and are, given the scope of the Principles, not dealt with.

(vi) Consumers, irrespective of the technology that is used to conclude contracts, must be treated on an equal footing. It must be irrelevant for consumer protection whether or not a particular technology is used. What matters is whether, from a functional viewpoint, a need for protection exists in light of a consumer's unequal bargaining position and any existing information asymmetry. The Principles do not deal with questions regarding extra-contractual liability in

---

3 See M Lehmann, National Blockchain Laws as a Threat to Capital Markets Integration, Uniform Law Review, Volume 26, Issue 1, March 2021, Pages 148–179.

4 See the European Commission's view on pan-European blockchain regulatory sandboxes in its statement on 'Shaping Europe's digital future' (<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-blockchain#:~:text=Pan%2DEuropean%20blockchain%20regulatory%20sandbox,that%20arise%20in%20deploying%20them> accessed 16 November 2022): 'A sandbox is a facility that brings together regulators, companies, and tech experts to test innovative solutions and identify obstacles that arise in deploying them. The European Blockchain Partnership is planning a pan-European regulatory sandbox in cooperation with the European Commission for use cases in the EBSI and outside of EBSI, including for data portability, B2B data spaces, SMART CONTRACTS, and digital identity (Self-Sovereign Identity) in the health, environment, mobility, energy and other key sectors. The sandbox is expected to become operational in 2021/22.' EBSI refers to the European Blockchain Services Infrastructure (<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI> accessed 16 November 2022).

5 <https://digital-strategy.ec.europa.eu/en/policies/blockchain-partnership> accessed 16 November 2022.

cases of software errors or the malfunctioning of a platform.[6] We also refer here to the work undertaken by another ELI Project Team that dealt with the model rules on online platforms.[7] However, it is obvious that in a rapidly digitalising world, the development of which was further enhanced by the Covid-19 pandemic, clarity needs to be ensured as to the rights of consumers when their counterparts make use of blockchain technology and Smart Contracts. Therefore, after presenting more general Principles, a set of special Principles is given specifically aimed at providing such clarity in the interests of the consumer. However, businesses too need more certainty as to what is expected from them. It is in everyone's interest that mutual rights and duties are clear, first of all protecting the position of consumers in an algorithmic environment, but also offering businesses clarity, enabling them to take consumer protection law into account when preparing further innovative initiatives.

The Principles follow an approach which is aimed at being both functionally equivalent to existing law and technologically neutral. To deal with the existing legal divergence in and outside Europe, the Principles are drafted in functionalist terms, avoiding jurisdiction-specific terminology as much as possible. Also, the Principles are formulated quite generally and in such terms that, in light of rapid technological advances, both the risks of under- and over-inclusion are avoided.

6 See the ELI Draft of a Revised Product Liability Directive: Draft Legislative Proposal of the European Law Institute (2022): <https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Draft_of_a_Revised_Product_Liability_Directive.pdf> accessed 16 November 2022.

7 See the ELI Report 'Model Rules on Online Platforms (2019)' <www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Online_Platforms.pdf> accessed 16 November 2022

Introductory Note

In the past 15 years we have seen a development towards an ever expanding digital economy next to the more traditional 'real' economy. This digital economy is based on several technological advances that are frequently characterised as disruptive technologies. An essential part of these technologies is DLT, of which blockchain technology is an application. The latter, in combination with the use of Smart Contracts, in a relatively short period of time has become widely applied. DLT makes it possible that all computers ('nodes') in a network are continuously synchronised in a decentralised way. Blockchain technology builds upon this by making it possible to create a 'block' of transactions the compilation and propagation of which is cryptographically connected to the previous such block (creating the 'chain'), so that each blockchain can have its own determinate transaction history and thus current balance. This is inter alia the basis for many cryptocurrencies, of which Bitcoin is the most well-known.

Smart Contracts are self-executing computer programmes, which can run on a blockchain,[8] facilitating transactions. After a period, often described as a 'hype cycle', during which it was predicted that blockchains and Smart Contracts could perhaps even replace trusted third parties, awareness has risen that these technologies have their specific technical limitations and cannot, as was once predicted, replace law by (computer) code.

A. Recent Developments with Regard to 'New Technologies' at European Level

Recently, the European Union published several packages of draft measures to create a legal framework for the hybrid world in which we now increasingly live: a world characterised by living simultaneously in the real and the digital economy. The proposed packages refer to the regulation of data governance ('Data Governance Act'),[9] crypto-assets ('Digital Finance Package'),[10] Artificial Intelligence ('Artificial Intelligence Act'),[11] digital services ('Digital Services Act'),[12] the digital market ('Digital Market Act'),[13] data sharing ('Data Act')[14] and measures against money laundering and terrorism financing.[15] The Digital

8 Smart Contracts can, of course, also be used outside blockchain technology as they only refer to a programme code containing an 'if-then' condition.

9 <https://digital-strategy.ec.europa.eu/en/policies/data-governance> accessed 16 November 2022.

10 <https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en> accessed on 16.11.2022.

11 <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_en#documents> accessed 16 November 2022; and <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence> accessed 16 November 2022.

12 <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en> accessed 16 November 2022.

13 <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en> accessed 16 November 2022.

14 <https://digital-strategy.ec.europa.eu/en/news/data-act-businesses-and-citizens-favour-fair-data-economy#:~:text=The%20Data%20Act%20will%20be,the%20support%20towards%20this%20initiative> accessed 16 November 2022.

15 Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast) (COM/2021/422 final): <https://eur-lex.europa.eu/resource.html?uri=cellar:08cf467e-ead4-11eb-93a8-01aa75ed71a1.0001.02/DOC_1&format=PDF> accessed 16 November 2022.

Finance Package contains a proposed regulation on markets in crypto-assets and is, as such, a first step towards creating a legal governance structure for the use of blockchain technology.[16] Also, the European Commission and the European Central Bank issued a joint statement about their cooperation on a digital euro.[17] With regard to a legal governance structure focusing more particularly on Smart Contracts, no initiatives have yet been taken.[18] This may change quickly, as the urgency not to leave these technologies unregulated has reached lawmakers and supervisory institutions, such as central banks, alike across the globe.[19]

In a period, labelled by the World Economic Forum as the 'Fourth Industrial Revolution', where the data economy is gaining a size equal to, or even surpassing, the more traditional economy, legal practice is faced with growing uncertainty about the legal nature, status and consequences of using blockchains and Smart Contracts. From what we have seen in practice, we understand that this uncertainty, in a

---

16 <https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0001.02/DOC_1&format=PDF> accessed 16 November 2022. See further on blockchains, the Study on Blockchains – Legal, Governance and Interoperability Aspects (SMART 2018/0038) <https://digital-strategy.ec.europa.eu/en/library/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038> accessed 16 November 2022. The European Commission is developing a blockchain strategy that also takes into account environmental concerns <https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy> accessed 16 November 2022.

17 Joint statement by the European Commission and the European Central Bank on their cooperation on a digital euro <https://ec.europa.eu/info/files/210119-ec-ecb-joint-statement-digital-euro_en> accessed 16 November 2022.

18 The EU Blockchain Observatory and Forum published a thematic report 'Regulatory Framework of Blockchains and Smart Contracts' (2019): <https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf> accessed 16 November 2022.
Regarding digital contracts, see <https://ec.europa.eu/info/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/digital-contract-rules_en> accessed 16 November 2022.

19 Providing a full and up-to-date overview of developments is no longer feasible. As a first brief entry to further information, the following (online) sources can be mentioned: An overview of developments in Europe is given by Matthias Lehmann, 'National Blockchain Laws as a Threat to Capital Markets Integration', Uniform Law Review/Revue de droit uniforme (2021), 1ff; for the United States, see the website of the National Conference of State Legislatures (NCSL) <www.ncsl.org/research/financial-services-and-commerce/blockchain-2021-legislation.aspx> accessed 16 November 2022. A more global overview can be found in Blockchain 2021, published by Chamber and Partners, with various authors each covering a particular jurisdiction, including, next to European jurisdictions, Australia, China, Hong Kong, Mexico, Russia, Singapore and the USA. See further, among others, the contributions in A Franceschi and R Schulze, *Digital Revolution – New Challenges for Law* (CH Beck/Nomos 2019), L DiMatteo, M Cannarsa and C Poncibò (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2020) and MC Compagnucci, M Fenwick and S Wrbka, *Smart Contracts. Technological, Business and Legal Perspectives* (Hart Publishing 2021). Recently published reports by the Law Commission of England & Wales and the Law Society of England & Wales are also highly relevant. See: the Law Commission's report on Smart Legal Contracts <www.lawcom.gov.uk/project/smart-contracts/> accessed 16 November 2022 and the Law Society's Blockchain: Legal and Regulatory Guidance (2nd edn) https://www.lawsociety.org.uk/topics/research/blockchain-legal-and-regulatory-guidance-second-edition> accessed 16 November 2022; A reference should also be made to two reports by the EU Blockchain Observatory & Forum, a report on Blockchain and Smart Contracts – Online workshop, March 10, 2022 (<https://www.eublockchainforum.eu/sites/default/files/reports/Workshop%20report_Blockchain%20and%20Smart%20Contracts.pdf> accessed 16 November 2022) and a report on Insights, Inputs and Recommendations to EU Blockchain Regulatory Efforts (<https://b-hub.eu/wp-content/uploads/2022/03/B-HUB_Report-on-insightsinputsrecommendations-to-EU-regulatory-efforts.pdf> accessed 16 November 2022). Finally, see the ELI Innovation Paper on Guiding Principles for Automated Decision-Making in the EU (2022) at https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Innovation_Paper_on_Guiding_Principles_for_ADM_in_the_EU.pdf accessed 16 November 2022.

way, slows down the use of new technologies as most commercial parties in the blockchain field (from startups to banks) do not want to risk non-compliance with applicable law and, thus, sometimes refrain from using new technologies.[20]

B. Why Principles on Blockchain Technology and Smart Contracts?

As outlined, DLT and blockchain technology has become widely applied. However, traditional legal doctrines on blockchain and Smart Contracts are not yet well developed, which results in significant legal uncertainty for all parties involved.

To enhance innovation, a legal framework is needed. Such a framework would clarify if, and if so, how and to what extent, blockchains and Smart Contracts may have legal implications. This aspect focusses on the use of these technologies from the perspective of existing law. However, a clear legal framework is also needed to clarify which limits the law must set as to the use of blockchains and Smart Contracts to avoid undesirable consequences, particularly, but not only, when consumers are involved.

As we believe that regulation and legal certainty *drive* innovation, in this report a set of Principles will be presented, which are aimed at providing a framework to create coordinated solutions among EU Member States and which might offer some support to other jurisdictions and international organisations which are also looking to create more certainty in this area.

These Principles aim at giving both academia and practitioners initial guidance on how to apply existing legal regulations to blockchain and Smart Contracts.

C. Structure of the Principles

a) ***Part I – General Part*****:** in the **General Part** of the report, Principles which apply more generally to questions regarding the legal implications of, for example, a transaction on a blockchain are presented. As such, the General Part applies to any type of transaction, whether in a commercial or a consumer setting.

b) ***Part II – Special Part on Smart Contracts and Consumer Protection*****:** consumers in particular may be confronted with the use of new technologies, which make it extremely difficult, not to say virtually impossible, for them to understand the nature of the transaction and its legal consequences. This implies that the situation of unequal bargaining power, against which consumer law has been developed, is even worse when disruptive technologies are used. In the

[20] See the website of the International Association for Trusted Blockchain Applications (INATBA), which, in several reports, explicitly refers to the importance of consumer protection (<https://inatba.org/> accessed 16 November 2022) and see, for the insurance industry, the discussion paper on blockchain and Smart Contracts in insurance published by the European Insurance and Occupational Pensions Authority (EIOPA) www.eiopa.europa.eu/sites/default/files/publications/consultations/eiopa-discussion-paper-on-blockchain-29-04-2021.pdf accessed 16 November 2022.

Special Part, therefore, Principles which are particularly aimed at giving consumers protection, at least equal to their protection under existing EU consumer law, are presented.

Black Letter Principles

Please note: words in capital letters refer to definitions at the beginning of the full text of the Principles (see pages 19–22).

I – General Principles

Principle 1 – Aim and Scope

a) The PRINCIPLES on BLOCKCHAIN technology and SMART CONTRACTS are intended for use in the European Union and elsewhere.
b) The PRINCIPLES are designed:
   (1) to establish a common understanding of aspects of BLOCKCHAIN technology and SMART CONTRACTS in the context of (civil) law;
   (2) to guide legal professionals when applying the existing legal framework to BLOCKCHAIN technology and SMART CONTRACTS;
   (3) if and where necessary to be a source to inspire further developments of the law by courts and the legislator; and
   (4) to inform the public about best practices as well as the application of law in the industry.
c) These PRINCIPLES only deal with the transactional aspects of BLOCKCHAINS and SMART CONTRACTS in as far as these can be qualified as being of a contractual nature.
d) These PRINCIPLES provide guidance within existing legal frameworks. These PRINCIPLES are not intended to amend or create any law. In case inconsistencies between these PRINCIPLES and other mandatory existing law occur, the mandatory existing law shall prevail if inconsistencies cannot be overcome by way of interpretation of the law.
e) The PRINCIPLES do not deal explicitly with:
   (1) the creation of rights *in rem*, such as a security right;
   (2) the proprietary effect of contracts;
   (3) legal or judicial enforcement;
   (4) questions regarding access to DIGITAL ASSETS in succession, matrimonial property or registered partnership property matters.

Principle 2 – Types of Smart Contracts

a) Various types of SMART CONTRACTS can be distinguished. A SMART CONTRACT can be:
   (1) mere CODE; no legal agreement exists (the situation is a mere TRANSACTION in the technical sense of the word);
   (2) a tool to execute a legal agreement; the legal agreement exists OFF-CHAIN;
   (3) a legally binding declaration of will, such as an offer or acceptance or constitute a legal agreement itself; or

(4) merged with the legal agreement and therefore exist simultaneously both ON-CHAIN and OFF-CHAIN.

b) If the SMART CONTRACT is merged with the legal agreement, it ought to be determined primarily by the parties whether the agreement should be treated as ON-CHAIN or OFF-CHAIN.

c) The PRINCIPLES focus on SMART CONTRACTS as a legally binding declaration (such as an offer or acceptance) and on SMART CONTRACTS as a legal agreement.

Principle 3 – Case Specific Approach

In the application of the PRINCIPLES it should, for each Principle and in each specific case, be considered which type of BLOCKCHAIN is used and who the parties involved are, and which type of SMART CONTRACT is used, as referred to in Principle 2.

Principle 4 – Private International Law

a) TRANSACTIONS made on or supported by BLOCKCHAIN technology are subject to the rules of the law that would apply to functionally equivalent acts outside the BLOCKCHAIN; this includes all rules of private international law.

b) According to generally accepted practice in international agreements, choice of law and choice of forum clauses can, generally, be validly agreed upon. Existing legal frameworks with regard to choice of law and choice of forum apply to TRANSACTIONS made on or supported by BLOCKCHAIN technology.

c) The mere fact that a BLOCKCHAIN, on which a SMART CONTRACT is stored, is decentralised, generally distributed and located in different countries does not, by itself, necessarily constitute an international dimension of said SMART CONTRACT in the sense of private international law.

d) Regarding Business to CONSUMER TRANSACTIONS, Principle 14 of the CONSUMER PRINCIPLES applies.

Principle 5 – Legal Nature of Transactions on a Blockchain

The triggering of TRANSACTIONS, or of elements of TRANSACTIONS, performed on a BLOCKCHAIN may amount to an offer, acceptance or any other contractual declaration where, depending on the specific nature of the SMART CONTRACT, such triggering can reasonably be understood as a declaration of will and is attributable to the relevant party.

Principle 6 – Effectiveness of an On-Chain Declaration of Will

a) The point in time at which a contractual declaration as mentioned in Principle 5 becomes effective should be contractually agreed upon between the parties.

b) In the absence of such agreement between the parties, an ON-CHAIN declaration of intent may only trigger legal consequences if:

(1) the recipient has actually received it; or
(2) the TRANSACTIONS are securely stored in the BLOCKCHAIN (ie cannot vanish in an orphan block).

Principle 7 – Formal and Substantive Validity

a) Rules concerning the formal and substantive validity of contracts under the applicable law apply to the conclusion of contracts on a BLOCKCHAIN; however, where the applicable law imposes formal requirements, the purpose of which is also fulfilled by the use of BLOCKCHAIN technology, without the applicable law explicitly referring to BLOCKCHAIN technology, the formal requirements should be deemed to have been fulfilled.

b) A text form can generally be replaced with BLOCKCHAIN technology or a SMART CONTRACT, whereas this might not apply to the condition of a written form if this implies a text document, either in writing on paper or in electronic format that is signed.

c) Formal requirements, such as the requirement that a contract must be in writing and signed, or needs to be drawn up in a particular format, such as an (authentic) deed, can only be fulfilled by a BLOCKCHAIN TRANSACTION or a SMART CONTRACT if the algorithmic representation of a written contract or deed equivalent to the OFF-CHAIN use of such requirements:

(1) guarantees the same safeguards;

(2) accomplishes the purpose of such formal requirements; and

(3) regarding electronic signatures, fulfils the requirements of the electronic IDentification, Authentication and trust Services (eIDAS) or an equivalent regulatory framework.

Principle 8 – Language

a) Contracts between businesses and between private parties can be concluded ON-CHAIN; the parties can also agree that the contractual language is a programming language.

b) For Business to CONSUMER contracts, Principle 15 of the CONSUMER PRINCIPLES applies.

Principle 9 – Off-Chain Prevails over On-Chain

Where a contract, or elements of a contract, concluded outside the BLOCKCHAIN, is translated into CODE (such as with a view to implementing the contract, or parts thereof, by automated means), the

terms of the contract concluded outside the BLOCKCHAIN prevail over any conditions coded on the BLOCKCHAIN, unless the parties have explicitly agreed otherwise.

Principle 10 – Unwinding by Reverse Transaction

Where the applicable law provides for the unwinding of a TRANSACTION, such unwinding shall normally occur by a REVERSE TRANSACTION unless the BLOCKCHAIN at hand allows for the modification of blocks.

Principle 11 – On-Chain Dispute Resolution Agreements

Arbitration agreements implemented in the respective executing SMART CONTRACT (eg as a 'comment') may be agreed upon between businesses. Such arbitration agreements may also agree upon a dispute resolution ON-CHAIN.

Principle 12 – Weaker Parties

WEAKER PARTIES shall be given the same or at least equal protection ON-CHAIN as they are entitled to OFF-CHAIN, from the perspective of both technological neutrality and functional equivalence, which must be adequate considering the algorithmic nature of a TRANSACTION.

II - Consumer Principles

Principle 13 – Consumer Protection Prevails Over and Fully Governs Coded Transactions

a) CONSUMER protection cannot be overridden by SMART CONTRACTS or any TRANSACTION on a BLOCKCHAIN.

b) If a CONSUMER TRANSACTION takes place using BLOCKCHAIN technology or a SMART CONTRACT, CONSUMER protection ON-CHAIN must be at least equivalent to the protection which a CONSUMER would have had if no such technology or SMART CONTRACT had been used.

c) Irrespective of the legal nature and contractual structure of a platform, the use of BLOCKCHAIN technology or a SMART CONTRACT shall not deprive CONSUMERS of any rights they might have had if the platform had not been used.

d) The immutability of a BLOCKCHAIN TRANSACTION or the automatic performance and execution of a SMART CONTRACT shall not deprive CONSUMERS of any right they would have had if an equivalent legally binding agreement had been concluded OFF-CHAIN.

e) Businesses using SMART CONTRACTS have to consider rights of weaker parties, such as CONSUMERS, before deploying SMART CONTRACTS and ensure that the rights of weaker parties can also be fulfilled ON-CHAIN (eg by way of reverse TRANSACTIONS or modifiable SMART CONTRACTS).

f) CONSUMERS relying on a previous ON-CHAIN TRANSACTION in good faith should be protected against OFF-CHAIN terms between businesses in the sense that any dealings between them ON-CHAIN are not binding or not binding on the same conditions as coded in the SMART CONTRACT.

Principle 14 – Private International Law and Consumer Transactions

Choice of law and choice of forum clauses contained in SMART CONTRACTS used by a business in its dealings with a CONSUMER are not to be given legal effect if a choice of law clause violates the rights of a CONSUMER regarding the otherwise applicable law or the choice of forum clause violates the right to sue or be sued before the courts of their country of habitual residence or domicile.

Principle 15 – Language and Consumer Transactions

Agreements regarding the use of programming language cannot be concluded between businesses and CONSUMERS. SMART CONTRACTS used for CONSUMERS always have to be translated into NATURAL LANGUAGE.

Principle 16 – Consumer Information Rights

a) CONSUMERS shall always have the same or functionally equivalent rights to information from their counterparts (including platform operators or similar service providers) as they would have had if no TRANSACTION on a BLOCKCHAIN or SMART CONTRACT had been performed.

b) This applies in particular to any pre-contractual information, but also to post-contractual information, such as part of a product recall, which a seller of goods or a supplier of services must give when the contract is not concluded using BLOCKCHAIN technology or a SMART CONTRACT.

c) Such information must always be available OFF-CHAIN, in natural, plain, intelligible and for the CONSUMER understandable language.

d) CONSUMERS are entitled to a translation and explanation of SMART CONTRACTS (both regarding procedure and substance) in natural, plain, intelligible and for the CONSUMER understandable language, in advance, updated whenever the SMART CONTRACT is updated, which must also be made available on a durable medium and publicly available on the user's website. If such translation and explanation are not made available, no legally binding

agreement results from the SMART CONTRACT, or, in the case of an update, the agreement can be terminated.

e) If the explanation deviates from the terms and conditions which apply once the contract has been concluded, the information contained in the explanation prevails or, if the deviation concerns essential characteristics of the contract, it may result in the contract being avoided.

Principle 17 – Duty to Code Cooling-Off (Consumer Right of Reflection or Right of Withdrawal)

(a) Whenever CONSUMERS are given the right to a cooling-off period such right must be:
  (1) coded into the SMART CONTRACT, to further protect CONSUMERS;
  (2) conferred in such a way that any right which a CONSUMER has regarding a cooling-off period can be exercised ON-CHAIN as OFF-CHAIN; and
  (3) communicated to the CONSUMER.

(b) A period of reflection shall be coded in such a way that the SMART CONTRACT only begins to execute in conformity with the applicable right to such a period.

(c) The SMART CONTRACT shall be programmed in such a way that when a CONSUMER exercises their right of withdrawal, the exercise of such right by itself results in a REVERSE TRANSACTION, taking into consideration the nature of the performance. If the nature of the performance prevents a REVERSE TRANSACTION, the CONSUMER may be entitled to a monetary claim representing the value of the TRANSACTION.

(d) The SMART CONTRACT shall be programmed in such a way that the CONSUMER is informed:
  (1) that the REVERSE TRANSACTION has taken place; and
  (2) that certain other rights, but also duties, might exist following the withdrawal.

(e) Coding a cooling-off period or a REVERSE TRANSACTION following the exercise of the right to withdrawal as part of the SMART CONTRACT will not be necessary if a CONSUMER would not be entitled to such a right, given, for example, the nature of the good, product or service.

Principle 18 – Unfairness Control (Unfair Terms) in Consumer Transactions

a) The protection of CONSUMERS against unfair terms shall be as effective ON-CHAIN as OFF-CHAIN.

b) A standard term that any agreement can only be concluded in digital format (ie ON-CHAIN, using SMART CONTRACTS) is, as such, not an unfair term.

c) CONSUMERS shall have the right to terminate a contract ON-CHAIN if it was concluded ON-CHAIN.

d) The provisions of the Unfair Terms Directive, and the *acquis communautaire* which has been developed around this Directive, shall be equally applicable as to whether a term in a SMART CONTRACT is unfair and, if so, which legal consequences this may have. The legally binding agreement shall then not contain the unfair term. In case the unfair term is a self-enforceable part of a SMART CONTRACT, the CONSUMER is entitled to immediate redress by having the contract re-coded.

e) Whenever a clause has been declared unfair in collective proceedings (such as under the Injunctions Directive or the Representative Actions Directive) a duty on the relevant business to re-code all SMART CONTRACTS affected arises.

Definitions

From Technical Definitions to Legal Definitions

In the context of new technologies, terms such as SMART CONTRACTS or BLOCKCHAIN are used in many settings. From our experience, different people very often mean different things when referring to such terms, eg a lawyer will very likely have a different understanding of a SMART CONTRACT than a software developer.

To ensure that the readers of this report share our understanding of the terms used, below we provide definitions of terms that we think are highly important.[21]

Term	Explanation
ASSET	Anything of value to a stakeholder.
BLOCKCHAIN TYPES	Software and architecture which are used in designing and delivering DLT systems which ordinarily, but not necessarily: 1. use a DISTRIBUTED LEDGER; 2. may be PUBLIC or PRIVATE or hybrids thereof; 3. are PERMISSIONED or PERMISSIONLESS or hybrids thereof; 4. are secure to a high level (using CRYPTOGRAPHY) against retrospective tampering, such that the history of TRANSACTIONS cannot be replaced; and 5. are auditable in the sense that there is a history of TRANSACTIONS.[22]

[21] The definitions used in the following are based on a mixture/combination of, or somewhat inspired by, the following sources: ISO Normalisation Work on Blockchains, Digital Ledger Technologies and Smart Contracts, published as ISO 22739:2020 (en) and English Law Commission, Smart Legal Contracts, Advice to Government (England and Wales) accessed on 11 January 2021 at <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf> accessed 16 November 2022. See also the consultation paper on digital assets, recently published by the English Law Commission: <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/07/Digital-Assets-Consultation-Paper-Law-Commission-1.pdf> accessed 16 November 2022. For early legislation within the European Economic Area, see the Innovative Technology Arrangements and Services Act 2018 of Malta, available at <https://legislation.mt/eli/cap/592/eng/pdf> accessed 16 November 2022, and the Token and TT Service Provider Act 2019 of Liechtenstein, available at <www.lcx.com/wp-content/uploads/2020_Liechtenstein_Blockcchain_Laws_Translation_English.pdf> accessed 16 November 2022. The definition of 'consumer' is based on the general approach to be found in European Union consumer law. For a further explanation, see the remarks at the beginning of Part II, the Special Part on Smart Contracts and Consumer Protection. See also M Hanzl, *Handbuch Blockchain und Smart Contracts* (Linde Verlag 2020).

BLOCKCHAIN(S)	A method of operating a DISTRIBUTED LEDGER. Data are typically stored in blocks organised in an append-only, sequential chain using cryptographic links to validate the integrity of historical data, with algorithmic validation of TRANSACTION logic and confirmation of the RECORDS by a defined mechanism for consensus among the NODES that process TRANSACTIONS.
CODE	Computational language that gives instructions to computers. A further distinction can be made between source code and bytecode. Source code could be readable to (some) human beings, whereas bytecode is typically not readable to human beings.
CONSUMER	Any natural person who is acting for purposes which are outside their trade, business, craft or profession.
CONSUMER PRINCIPLES	CONSUMER-related PRINCIPLES 13–18 as outlined in Part II of this report.
CRYPTO-ASSET	A digital representation of value or rights which may be transferred and stored electronically, using DLT or similar technology (Article 3(2) Draft MiCA).
CRYPTOCURRENCY	See VIRTUAL CURRENCY.
CRYPTOGRAPHY	Discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorised use, or prevent their undetected modification.
DECENTRALISED AUTONOMOUS ORGANISATION (DAO)	An organisation, encoded as a computer programme on a BLOCKCHAIN, facilitated by SMART CONTRACTS, operating based on votes by members holding digital tokens of their membership.
DIGITAL ASSET	See CRYPTO-ASSET.
DISTRIBUTED LEDGER	A store of data that is intended to be final, definitive and immutable, where the store is shared across a network of computers (NODES).
DISTRIBUTED LEDGER TECHNOLOGY (DLT)	A type of technology that supports the distributed recording of encrypted data. A BLOCKCHAIN is a sub-category of DLT.
GENERAL PRINCIPLES	PRINCIPLES 1–12 as outlined in Part I of this report.
NATURAL LANGUAGE	Language used between people to communicate (eg English, French, German).
NODE(S)	Device or process that participates in a DISTRIBUTED LEDGER network.

[22] See also Innovative Technology Arrangements and Services Act 2018, definition of 'innovative technology arrangements', available at <https://legislation.mt/eli/cap/592/eng/pdf> accessed 16 November 2022.

	Nodes can store a complete or partial replica of the DISTRIBUTED LEDGER.
OFF-CHAIN	Located, performed or run outside a BLOCKCHAIN system.
ON-CHAIN	Located, performed or run inside a BLOCKCHAIN system.
ORACLE	Service that updates a DISTRIBUTED LEDGER (eg a BLOCKCHAIN) using data from outside a DISTRIBUTED LEDGER system (outside the BLOCKCHAIN context). An ORACLE transmits OFF-CHAIN information in a computer-readable form to the network.
PERMISSIONED DISTRIBUTED LEDGER SYSTEM	DISTRIBUTED LEDGER system wherein its NODES need authorisation to perform certain activity or activities, in particular the processing of TRANSACTIONS.
PERMISSIONLESS DISTRIBUTED LEDGER SYSTEM	DISTRIBUTED LEDGER system wherein its NODES do not need authorisation to perform any activity or activities, in particular the processing of TRANSACTIONS.
PRINCIPLES	PRINCIPLES in Part I and Part II of this report (Principle 1 – Principle 18).
PRIVATE DISTRIBUTED LEDGER SYSTEM	DISTRIBUTED LEDGER system in which a controlled and limited set of NODES participate in the operation of the system.
PUBLIC DISTRIBUTED LEDGER SYSTEM	DISTRIBUTED LEDGER system in which participation (as a NODE) in the operation of the system is not controlled or limited.
RECORD(S)	Information created, received and maintained as 'evidence' and as an ASSET by an organisation or person, in pursuit of legal obligations or in a business transaction. The term 'evidence' is not limited to the legal sense. This applies to information in any medium, form or format.
REVERSE TRANSACTION	REVERSE TRANSACTIONS are opposing TRANSACTIONS whereby the originally executed TRANSACTION is reversed by a subsequent, exactly opposing TRANSACTION. Usually such TRANSACTIONS are necessary in cases of void or revoked TRANSACTIONS to ensure that the factual state on the BLOCKCHAIN corresponds to the legal state after the exercise of a right of revocation or in the case of a void TRANSACTION.
SMART CONTRACT	Computer programme that, upon the occurrence of pre-defined conditions, runs automatically and executes pre-defined actions. A SMART CONTRACT may or may not be intended to represent terms in a contract in law or be legally recognised. This definition considers SMART CONTRACTS only in the context of DISTRIBUTED LEDGER SYSTEMS. It is recognised that SMART CONTRACTS are not restricted to DISTRIBUTED LEDGER SYSTEMS and the term may have a different meaning in other

	contexts.
TRANSACTION	A TRANSACTION on a BLOCKCHAIN refers to an action on the BLOCKCHAIN which results in a change of state on the BLOCKCHAIN (eg a transfer of CRYPTOCURRENCY comprising a reduction of the amount of CRYPTOCURRENCY the owner of private key A can dispose of and an increase of the amount of CRYPTOCURRENCY the owner of private key B can dispose of).
VIRTUAL CURRENCY	A digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.[23]
WALLET	Mechanism for storing private and public keys that enables DLT users to transact.
WEAKER PARTY	A WEAKER PARTY in the context of these PRINCIPLES could be anyone that is typically in a weaker position to negotiate for themselves (eg a CONSUMER, an employee, a tenant, or micro-, small- or medium-sized enterprise).

[23] Article 3(18) of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

1 PART I – GENERAL PART

1.1 Principles

Principle 1 – Aim and Scope

a) The PRINCIPLES on BLOCKCHAIN technology and SMART CONTRACTS are intended for use in the European Union and elsewhere.
b) The PRINCIPLES are designed:
   (1) to establish a common understanding of aspects of BLOCKCHAIN technology and SMART CONTRACTS in the context of (civil) law;
   (2) to guide legal professionals when applying the existing legal framework to BLOCKCHAIN technology and SMART CONTRACTS;
   (3) if and where necessary to be a source to inspire further developments of the law by courts and the legislator; and
   (4) to inform the public about best practices as well as the application of law in the industry.
c) These PRINCIPLES only deal with the transactional aspects of BLOCKCHAINS and SMART CONTRACTS in as far as these can be qualified as being of a contractual nature.
d) These PRINCIPLES provide guidance within existing legal frameworks. These PRINCIPLES are not intended to amend or create any such law. In case inconsistencies between these PRINCIPLES and other mandatory existing law occur, the mandatory existing law shall prevail if inconsistencies cannot be overcome by way of interpretation of the law.
e) The PRINCIPLES do not deal explicitly with:
   (1) the creation of rights *in rem*, such as a security right;
   (2) the proprietary effect of contracts;
   (3) legal or judicial enforcement;
   (4) questions regarding access to DIGITAL ASSETS in succession, matrimonial property or registered partnership property matters.

Explanatory Notes

The Principles, as presented below, are intended to serve as general guidelines, which give a first orientation for the handling of blockchain technology and Smart Contracts from a private law perspective. In the Explanatory Notes, the possible solutions *de lege ferenda* will be identified. The EU *acquis communautaire* and draft EU legislative measures were considered, next to developments in national law. When drafting the Principles, it was clearly apparent that fundamental differences may exist between B2B, B2C, G2G, B2G and G2C transactions. Also, the Principles fully respect data strategies and resulting policies as put forward by European law with regard to both privacy and data protection,

the free flow of non-personal data and the possible sharing of non-personal data between professional parties and governments.[24]

The scope of the Principles is limited from several perspectives. First of all, the focus is on the private law aspects of the use of blockchains and Smart Contracts, not on the public regulatory or sandbox aspects. However, as Smart Contracts, from a technical perspective, always constitute 'if-then' conditions, it is necessary to analyse Smart Contracts on a case-by-case basis to determine whether a specific Smart Contract touches upon civil law aspects and, thus, falls within the scope of these Principles. As a guidance hereto, we have established four 'types' of Smart Contracts from a legal perspective as outlined in Principle 2, recognising that, from a technical perspective, there is only one 'type'. Secondly, the Principles deal with transactions on the blockchain, meaning an action on the blockchain, which results in a change of state on the blockchain (eg the 'transfer' of cryptocurrencies, which leads to a reduction of the amount of cryptocurrency that the owner of private key A can dispose of, and an increase of that amount for the owner of private key B). Furthermore, these transactions should be of a contractual nature. The latter includes the entire 'life cycle' of a contract, which means from contract formation (including the pre-contractual stage), through performance, to the post-contractual stage. A transaction can be an invitation to treat, an offer or acceptance, performance and execution, and any services to be provided after performance. Excluded are, therefore, the creation of rights *in rem*, such as a security right, the proprietary effects of contracts, legal or judicial enforcement and questions regarding access to digital assets in matters of succession, matrimonial property or registered partnership property. The ELI has already published a report on the Use of Digital Assets as Security.[25] A second report on enforcement is currently being drafted. If, according to a particular legal system, a contract has a proprietary effect, the resulting questions are outside the ambit of these Principles. However, a legal system should then take great care to ensure that any requirements as to, for example, registration, which must be fulfilled before any proprietary consequences may follow in particular for third parties in good faith, are complied with following the *lex registrationis*.

---

[24] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), [2002] OJ L201/37 (to be replaced by a Regulation on Privacy and Electronic Communications); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L119/1, Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, [2018] OJ L303/59 and Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), [2019] OJ L172/56 (replacing, from 17 July 2021, Directive 2003/98/EC of the European Parliament and of the Council, OJ L345/90 and Directive 2013/37/EU of the European Parliament and of the Council, OJ L175/1). See also the Communication from the Commission to the European Parliament and the Council Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union (COM(2019) 250 final). See also the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Towards a common European data space ((SWD(2018) 125 final), COM(2018) 232 final), the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A European strategy for data (COM(2020) 66 final), and the Data Governance Act (Proposal for a Regulation of the European Parliament and of the Council on European data governance, COM(2020) 767 final).

[25] See ELI Principles on the Use of Digital Assets as Security, Report of the European Law Institute (2022): <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_the_Use_of_Digital_Assets_as_Security.pdf> accessed 16 November 2022

Principle 2 – Types of Smart Contracts

a) Various types of SMART CONTRACTS can be distinguished. The SMART CONTRACT can be:
   (1) mere CODE; no legal agreement exists (the situation is a mere TRANSACTION in the technical sense of the word);
   (2) a tool to execute a legal agreement; the legal agreement exists OFF-CHAIN;
   (3) a legally binding declaration of will, such as an offer or acceptance or constitute a legal agreement itself; or
   (4) merged with the legal agreement and therefore exist simultaneously both ON-CHAIN and OFF-CHAIN.
b) If the SMART CONTRACT is merged with the legal agreement, it ought to be determined primarily by the parties whether the agreement should be treated as ON-CHAIN or OFF-CHAIN.
c) The PRINCIPLES focus on SMART CONTRACTS as a legally binding declaration (such as an offer or acceptance) and on SMART CONTRACTS as a legal agreement.

Explanatory Notes

Descriptive nature: this Principle is of a descriptive nature, as it outlines and illustrates the different types of Smart Contracts. As outlined in Principle 1, these Principles focus on contractual aspects of Smart Contracts. Thus, the Principles focus on Smart Contracts as outlined in Principle 2 a)(3) and (4). However, in practice, we see that the various types of Smart Contracts are being used. Hence, to determine the applicability of these Principles, the distinction in Principle 2 is necessary.

Blockchain technology: a blockchain is a decentralised technology. As decentralisation is one of the main characteristics of blockchain technology and a considerable number of (legal) questions are related thereto, we assume that the Principles can also be applied to other DLTs. However, we acknowledge that there may be areas where this is not feasible due to technological changes. In such cases, specific principles or rules will have to be adopted.

Even if this report often refers to 'the blockchain' or 'the blockchain technology', it is well understood that there is not only 'one' blockchain, but many variations thereof.

In general, a blockchain can be classified as either a private or public blockchain as well as permissioned or permissionless.

From a legal perspective, the distinction between private and public blockchain is essential. A private blockchain is a blockchain in which only certain persons can participate. Before participation in the blockchain, the respective (personal) participation requirements are usually checked by the (central) gatekeeper. The users of a private blockchain are often identifiable (mostly by the gatekeeper, sometimes also by other users of the blockchain). Further, the nodes operating the blockchain are usually known. Thus, the operation of the blockchain can be interfered with. A public blockchain is a blockchain which can be joined at any time by downloading the publicly available client (provided the

technical requirements are met). There is neither a check of requirements by a gatekeeper nor authentication of the individual participants of the blockchain.

A further distinction can be made between permissioned and permissionless blockchains. This subdivision is aimed in particular at the issue of authorisations. In the case of permissioned blockchains, only certain people are allowed to execute transactions on the blockchain, whereas, in the case of permissionless blockchains, anyone is allowed to execute transactions on the blockchain.

There are therefore four main types, namely: (1) public permissioned blockchains; (2) public permissionless blockchains; (3) private permissioned blockchains; and (4) private permissionless blockchains.

The parties to blockchain transactions can be businesses, governments and/or consumers. The legal status, and consequently the bargaining positions and knowledge levels, varies considerably both between and within these groups. In many respects, small- and medium-sized enterprises (SMEs) have a far weaker position than, for example, large international business enterprises or governments and government agencies. This applies even more so to consumers, whose position in DLT transactions is extremely weak. Consumer protection must at least be at the same level on-chain as it is off-chain, given the asymmetrical knowledge, information and bargaining position between consumers and businesses as well as consumers and governments. This also applies to other weaker parties, such as tenants and employees. However, the Principles as such will more specifically focus (see Part II of these Principles) on the protection of consumers.

Source code and bytecode: in discussions about possible legal implications of using Smart Contracts, a distinction between source code and bytecode might be made. Source code is human-readable programming language, bytecode is generated from source code and, generally speaking, not human readable. Source code is off-chain, as is the use of natural language; bytecode is on-chain. Whenever it seemed necessary in the Explanatory Notes, the two types of code are distinguished. A further distinction is not made.

Smart Contracts are self-executing computer programmes: Smart Contracts are a much-discussed topic in legal literature, which is partially caused by their name. When lawyers think of 'contracts', they immediately think of legally binding agreements, although this is not necessarily what coders mean.

From a purely technical perspective, Smart Contracts are programme codes that represent 'if-then' conditions. From a legal perspective, the question is whether these programme codes can be contracts under civil law.[26] This question cannot be answered by presenting a hard and fast rule. A careful case-by-case analysis will be needed, given the differences in types of blockchains, parties and interests involved. Nevertheless, certain fairly general guidelines can be given. Such rules have the advantage that they provide certainty *ex ante*, clarity already when the contract is at a stage of formation, but may be over- or under-inclusive in their practical impact and, therefore, may result in an unfair outcome. A case-by-case analysis has the advantage of providing flexibility to courts and arbitrators, so fairness *ex post*, after the formation of the contract and at the stage that it is performed, but results in uncertainty. Given that the technologies on which these Principles focus are new and still in continuous development, a balance

[26] Cf M Durovic and A Janssen, 'The Formation of Blockchain-based SMART CONTRACTS in the Light of Contract Law' (2019) European Review of Private Law 753ff.

has to be struck between *ex ante* certainty and *ex post* fairness. Guidelines, presented as Principles, appear to be the most suitable means of achieving such a balance; the most important guideline being that Smart Contracts can also be binding under civil law.[27] The Principles take the traditional requirements for a validly binding agreement as their starting point.[28] A contract comes into existence when the declarations of intent of two parties match. In other words, a contract is concluded if the offer and acceptance are congruent. Offer and acceptance here are given the meaning as generally accepted in traditional contract law. A legally valid offer must be sufficiently specific in terms of content and the offeror must express sufficient intent to be bound. However, a mere invitation to make an offer is different from an offer; this is always the case when no sufficient intention to be bound is expressed for an offer. A valid acceptance must be in agreement with the offer; the acceptance must therefore not deviate from the offer.

Although a case-by-case approach is advocated in these Principles, the following scenarios can still be identified:[29]

2(a)(1) The SMART CONTRACT can be mere code; no legal agreement exists (the situation is a mere TRANSACTION in the technical sense of the word).

As explained, Smart Contracts are 'if-then' terms. Therefore, there may also be cases in which Smart Contracts merely perform status changes on the blockchain that lead to *de facto* changes without any further legal effect. Such Smart Contracts are not contracts in the civil law sense, but merely technical phenomena.

Voting in a Decentralised Autonomous Organisation (DAO) Use Case

There are different models for DAO memberships that can determine how voting works. However, in many cases, a DAO is fully permissionless and decisions are made by using governance tokens. Every holder of a governance token can exercise their voting right.

From a technical point of view, this usually happens with support of transactional (voting) Smart Contracts. Typically, a token holder will make a proposal to the DAO members. The token holders can then vote on the proposal by, eg transferring their governance token to said Smart Contracts (either pro or against the proposal). After the voting process, every token holder has their governance token returned.

The execution of a voting Smart Contract is purely transactional and, thus, does not constitute a legally binding contract.

---

27 This guideline is further elaborated upon from the perspective of blockchain transactions as such in Principle 5 and Explanatory Notes to Principle 5.

28 For a restatement as to how, within the EU, contract formation is approached see Ch Bar, E Clive and H Schulte Nölke (eds), *Principles, Definitions and Model Rules of European Private Law. Draft Common Frame of Reference (DCFR, Outline Edition)* (Sellier 2009), Articles II.-4:101ff and Ch Bar and E Clive, *Principles, Definitions and Model Rules of European Private Law. Draft Common Frame of Reference (DCFR, Full edition)*, Vol I (Oxford University Press 2010), 125ff.

29 The Reporters would like to thank Jasper Verstappen, LLB, LLM, member of the project team, for allowing them to make use of his, at the moment of publication of this report, unpublished PhD research regarding the above classification of Smart Contracts.

2(a)(2) The SMART CONTRACT can be a tool to execute the legal agreement; the legal agreement exists OFF-CHAIN.

In this case, a legally binding contract is concluded outside the blockchain system ('off-chain'). In this off-chain contract, the rights and obligations of the contracting parties are defined and it is already agreed that blockchain technology, or more precisely Smart Contracts, will be used to execute the contract.

The Smart Contracts used in this case are merely acts of performance or settlement tools. However, these Smart Contracts are not binding contracts under civil law.[30]

Certainly, in this context, there may be challenging legal issues (such as under what circumstances blockchain technology can be used to fulfil contracts, who bears the risk of poor performance of a Smart Contract?, etc). However, these issues can be resolved using the general principles of civil law.

Flight Insurance Use-Case

In 2017, an insurance group launched an insurance product, which was partially blockchain-based.

In this scenario people could basically conclude a flight delay insurance policy online (via a 'classic web interface'). Once such an insurance agreement was concluded by and between the insurer and a customer, a self-executing Smart Contract automatically executed such an agreement. Customers would not have to manually trigger insurance coverage in the case of a flight delay, since the Smart Contract would automatically check if the insureds' flight was late according to the policy terms and, if so, would initiate an automated pay-out.

For example, in the case of a two-hour flight delay, the Smart Contract would automatically initiate a pay-out of the pre-defined sum (the if-then condition of the Smart Contract would basically just check: 'if flight is delayed more than two hours, then pay-out has to be initiated').[31]

Such a Smart Contract is the mere execution of an off-chain concluded contract (in this case the insurance agreement).

However, this use-case should not be confused with other 'insurance' cases in the context of decentralised finance potentially concluded on-chain via Smart Contracts.

2(a)(3) The SMART CONTRACT can be a legally binding declaration of will, such as an offer or acceptance or constitute a legal agreement itself.

When analysing the formation stage leading towards a contract, it could very well happen that only a part of that stage is concluded by making use of Smart Contracts. The Smart Contract (and again the use of the word contract shows how unfortunate that term here is from a legal perspective) could be the

[30] P Filippi, Ch Wray, G Sileno, *Smart Contracts*, accessed on 30 May 2021 at <https://policyreview.info/glossary/smart-contracts> accessed 16 November 2022; Rupa, 'Standardisierte Projektverträge als Smart Contracts. Computergestützte Automatisierung eines Vertrages am Beispiel der FIDIC-Bedingungen' (2021) MMR, 371; Mann, (2017) NZG 1015; Ch Buchleithner, T Rabl, ecolex (2017) 6; M Hanzl, *Handbuch Blockchain* (2020), 44; S Smets, S Kapeller, (2018) ÖJZ 294.

[31] Please note, that in such use-cases, the on-chain world (flight delay Smart Contract) of course has to be linked to the off-chain world (the actual information as to whether a flight was delayed). This could be done via ORACLES.

offer, which is accepted off-chain (for example, because of written or verbal communication), or the on-chain acceptance of an offer that itself is off-chain. In the latter situation, an offer is made off-chain, eg in the form of a source code; acceptance takes place on-chain when the other party compiles the source code into bytecode and deploys it to the blockchain. Note, however, that if the first party now fails to interact with the bytecode (eg by transferring cryptocurrency to the address at which the bytecode is deployed), this is a breach of contract, although this may sound almost counterintuitive. It is worth making it clear that these Principles, particularly when focusing on consumer protection, also apply when the Smart Contract cannot be qualified as a legal agreement, but consists of elements which result in such an agreement.

In light of the above, the question arises as to whether Smart Contracts, ie the programme code, can constitute legally binding declarations. Ultimately, the underlying legal question is whether declarations of intent can be expressed by a programme code.[32]

It is submitted that – as an outflow of private autonomy – a Smart Contract should be an eligible way to express the will of a party.[33] However, this should certainly not lead to a reduction of the protection of market participants or consumers, ie all remedies (eg moral unlawfulness remedies, consumer protection rules) also apply in the context of Smart Contracts.

A Smart Contract stored on a blockchain can also generally fulfil the requirements of an offer, namely the definiteness of the content and the intention to bind:

i. Given the 'if X, then Y-condition' of the Smart Contract, it must already be clear when the Smart Contract is deployed which performance is owed if the Smart Contract is triggered, eg by payment of a cryptocurrency amount. As a result, the Smart Contract will generally be determined in terms of its content; and
ii. Binding intention is also generally given by the storage on the blockchain, since, after storage on the blockchain, a Smart Contract can no longer be changed due to the characteristics of the blockchain.

Thus, a Smart Contract can constitute an offer in the legal sense. Such an offer may be accepted by implication.

Potential objection as to compilation of source code to bytecode: from a technical perspective, Smart Contracts are a set of instructions in the form of bytecode. Thus, before executing a Smart Contract on a blockchain network, the – potentially human readable – source code has to be compiled into machine-readable bytecode.[34] **A misconception could arise that because of the need to compile source code into bytecode, source code cannot represent the content of a – potentially – legally relevant Smart**

---

[32] This question has been heavily discussed in legal literature. See for an example of the debates at national level, arguing in favour of Smart Contracts potentially being legally binding contracts: S Smets, S Kapeller, *Smart Contracts: Vertragsabschluss und Haftung*, ÖJZ 2018/ 39 (293f); *Schmidt* in *Schmidt*, Kryptowährungen und Blockchains 122; M Hanzl, T Rubey, *Smart Contracts – die intelligente Art Verträge zu schließen?*, Zak 2018/238 (128ff); M Hanzl, *Handbuch Blockchain und Smart Contracts* (2020) 87; Ch Buchleitner T Rabl, *Blockchain und Smart Contracts*, ecolex 2017, 4; arguing against it E Welten*, B* Ozsvar in *Binder Grösswang*, Digital Law (2018) Zivilrecht, 15f.

[33] M Hanzl*, Handbuch Blockchain und Smart Contracts* (2020), 104ff.

[34] P Filippi, Ch Wray, G Sileno, 'Smart Contracts', accessed on 30 May 2021 at <https://policyreview.info/glossary/smart-contracts> accessed 16 November 2022.

Contract: this is not the case, because although the 'translation' of the contract terms from source into bytecode is necessary, the source code still determines the bytecode and thus also the key elements of the Smart Contract. Insofar as errors occur in the translation of source into bytecode (for example, because the compiler is defective), these translation errors must be resolved in accordance with general civil law provisions. In practical terms, this would mean that if person A wants to make an offer on the blockchain using a Smart Contract and programmes a Smart Contract in source code for this purpose, defining the key elements of the offer, person A generally only wants to be bound by this offer. If the offer is now misrepresented due to a faulty compilation of the source code in bytecode, whether person A should be bound to the (faulty) offer expressed in bytecode must be reviewed according to general civil law regulations.

To conclude, a Smart Contract can be regarded as (part of) a legally binding agreement, provided that the prerequisites for the conclusion of a contract in the respective legal system (eg offer and acceptance) are fulfilled.[35] This conclusion is two-fold. First, when analysing the relationship between negotiating parties, the use of source code or bytecode does not by itself prevent any conclusion that they created a legally binding agreement. Second, following the well-established rules on contract formation, a declaration of will could very well be expressed in coded format. It cannot be denied that, in practice, numerous and difficult to resolve problems may come up. For example, consider the situation where two commercial parties have a history of implementing their off-chain legal agreement using bytecode on a blockchain, without reference to any source code and one party deploys the same, familiar bytecode with the intention that the other party would be able to accept it as legally binding simply by interacting with the bytecode, eg by transferring cryptocurrency to the address at which the bytecode is deployed. In this case, although their history might lead a court to imply terms by custom and practice (the terms expressed in the source code exchanged on previous occasions), it could reasonably be argued that both parties communicated their legally binding intentions solely through bytecode.

Initial Coin Offerings (ICOs) Use Cases

One case in which a Smart Contract can constitute an offer and a corresponding transaction can constitute the acceptance might be initial coin offerings (ICO), others might be decentralised exchanges, crypto lotteries or the like.

With regard to an ICO, typically a Smart Contract that issues the new tokens will be deployed on a BLOCKCHAIN, stating, simplified, 'If someone transfers 0.1 ETH to this Smart Contract address, they will receive one newly minted token'.

[35] Cf R de Caria, *The Legal Meaning of Smart Contracts* (2019) European Review of Private Law, 731ff; M Di Angelo, A Soare, G Salzer, *Smart Contracts in View of Civil Code*, at <https://publik.tuwien.ac.at/files/publik_278278.pdf> accessed 16 November 2022; Levi/Lipton, 'An Introduction to Smart Contracts and their Potential Inherent Limitations' Harvard Law School Forum on Corporate Governance, accessed on 30 May 2021 at <https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/> accessed 16 November 2022; S Smets, S Kapeller, *Smart Contracts: Vertragsabschluss und Haftung* (2018/39) ÖJZ 293f; *Schmidt* in *Schmidt*, Kryptowährungen und Blockchains 122; M Hanzl, T Rubey, *Smart Contracts - die intelligente Art Verträge zu schließen*?, Zak 2018/238 (128ff); M Hanzl, *Handbuch Blockchain und Smart Contracts* (2020) 87; Ch Buchleitner, T Rabl, *Blockchain und Smart Contracts*, ecolex 2017, 4.

Depending on the concrete circumstances, prima vista, the deployment of such a Smart Contract can constitute a legally binding offer as it contains the necessary information (ie the price of the newly issued token and the description of the good to be purchased (namely the newly issued token)). Such an offer could then be accepted by transferring money to the Smart Contract.

2(a)(4) The SMART CONTRACT is merged with the legal agreement and therefore exists simultaneously both ON-CHAIN and OFF-CHAIN; in the latter situation, it ought to be determined whether the agreement should be treated as ON-CHAIN or OFF-CHAIN.

In the case of a conflict between the OFF-CHAIN and the ON-CHAIN version of the contract, following Principle 9 below, the OFF-CHAIN text prevails. Still, the contract is of a hybrid nature, which may, from a legal viewpoint, affect its formation, content, performance and enforcement. This is particularly relevant in cases of so-called 'Ricardian contracts', developed by Ian Grigg in 2000 as contracts which are both readable on paper and readable by computer programmes.[36]

Principle 3 – Case Specific Approach

In the application of the PRINCIPLES, it should, for each Principle and in each specific case, be considered which type of BLOCKCHAIN is used and who the parties involved are and which type of SMART CONTRACT is used, as referred to in Principle 2.

Explanatory Notes

As elaborated above, four 'main types' of blockchain technology can be identified, namely public permissionless, public permissioned, private permissionless, and private permissioned.[37]

The choice of blockchain type for a particular transaction can have far-reaching consequences, for example, certain legal obligations (eg obligations under the EU's General Data Protection Regulation)[38] can be implemented more easily on private blockchains controlled by a few nodes, while such blockchains admittedly do not embody the original idea of the blockchain.

Principle 4 – Private International Law

a) TRANSACTIONS made on or supported by BLOCKCHAIN technology are subject to the rules of the law that would apply to functionally equivalent acts outside the BLOCKCHAIN; this includes all rules of private international law.
b) According to generally accepted practice in international agreements, choice of law and choice of forum clauses can, generally, be validly agreed upon. Existing legal frameworks with regard to choice

36 U W Chohan, *What Is a Ricardian Contract?* (11 December 2017). Available at SSRN: <https://ssrn.com/abstract=3085682> accessed 16 November 2022 or <http://dx.doi.org/10.2139/ssrn.3085682> accessed 16 November 2022.

37 D Saive, CR 2018,187.

38 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

of law and choice of forum apply to TRANSACTIONS made on or supported by BLOCKCHAIN technology.

c) The mere fact that a BLOCKCHAIN, on which a SMART CONTRACT is stored, is decentralised, generally distributed and located in different countries does not, by itself, necessarily constitute an international dimension of said SMART CONTRACT in the sense of private international law.

d) Regarding Business to CONSUMER TRANSACTIONS, Principle 14 of the CONSUMER PRINCIPLES applies.

Explanatory Notes

When assessing facts with a cross-border element, private international law must be taken into account for the identification of which law is applicable to the specific facts. Decisive for the applicability of private international law is the existence of a 'cross-border element'.[39]

In the context of blockchain and Smart Contracts, it is debatable when such a cross-border element exists.

In our view, and following a functional approach, the rules of private international law do not *per se* apply to Smart Contracts that are stored in a decentralised manner across multiple countries. The mere fact that the nodes processing the transactions are distributed across multiple countries does not automatically lead to Smart Contracts having cross-border elements. If an online transaction, eg in an online store, between two citizens of one country is hosted via a server located in another country, this also does not lead to the application of private international law. In our opinion, the same should apply to Smart Contracts. Consequently, the rules of private international law are only applicable if there is a further foreign connection (eg, the contracting parties are resident in different countries).[40]

This could be somewhat different in connection with the question of the applicability of private international law to blockchains. To the extent that the nodes joining the blockchain are from different countries, this could constitute a sufficient cross-border element for the application of private international law.

Of course, it could be debated what 'functionally equivalent acts outside the BLOCKCHAIN' are and which more concrete rules then could or should apply. For the time being, a rather pragmatic and more problem-based approach seems to be the best way forward, as can also be recognised in the various legislative packages updating and reforming EU law in the area of the digital economy. An example can be found in the ELI report on the Use of Digital Assets as Security, in which more concrete choices were made as to the law governing such specific arrangements, taking into account both the position of the parties to a security agreement and the position of third parties.[41]

It is commercial practice to include in an international agreement a choice of law and choice of forum clause. Such clauses, however, are not always allowed. Several well-recognised exceptions exist, such as

---

39 B Lurger, M Melcher, *Handbuch Internationales Privatrecht* (2017), § 1 Allgemeine Fragen, Rz 1/1.

40 M Hanzl, *Handbuch Blockchain*, 60f.

41 ELI Principles on the Use of Digital Assets as Security, available at < https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_the_Use_of_Digital_Assets_as_Security.pdf> accessed 16 November 2022.

when the applicable law violates public policy (*ordre public*) or when mandatory rules of an international nature (*règles d'application immédiate*) apply. Examples of public policy violations are tax evasion, money laundering, financing of terrorist activities or avoidance of international embargos. Another example of when a choice of law clause will not be effective is when it bypasses the law applicable to the transfer of an immovable property where the *lex rei sitae* and *lex registrationis* are leading. Exceptions also exist to protect weaker parties. Regarding the protection of consumers against abusive choice of law and choice of forum clauses in an algorithmic environment, see CONSUMER PRINCIPLES.

Principle 5 – Legal Nature of Transactions on a Blockchain

The triggering of TRANSACTIONS, or of elements of TRANSACTIONS, performed on a BLOCKCHAIN may amount to an offer, acceptance or any other contractual declaration where, depending on the specific nature of the SMART CONTRACT, such triggering can reasonably be understood as a declaration of will and is attributable to the relevant party.

Explanatory Notes

Legal nature of blockchain transactions: this Principle was at the heart of several rounds of discussion among the Reporters and within the whole Project Team. The final conclusion was that the approach taken in Principle 5 is, indeed, accurate and reflects existing law, not only in B2B and B2G, but also in B2C relations. For commercial, financial and government relations, no doubts existed, given international practice, but the issue of how to ascertain existing and future consumer protection in particular was a point of grave concern. However, by formulating Principles specifically aimed at protecting consumers (see Part II of these Principles), the Project Team agreed that consumer protection could be more than adequately safeguarded.

The discussions as to whether TRANSACTIONS or elements thereof can amount to an offer, acceptance or any other contractual declaration, centred around the European Parliament resolution of 20 October 2020 with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL)) and Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights.[42] In this resolution, the European Parliament requests the European Commission:

> 'to in particular update its existing guidance document on Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights in order to clarify whether it considers smart contracts to fall within the exemption in point (l) of Article 3(3) of that Directive, and, if so, under which circumstances, and to clarify the issue of the right to withdrawal.'

[42] See <https://www.europarl.europa.eu/doceo/document/A-9-2020-0177_EN.html> accessed 16 November 2022, page 7 and Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, [2011] OJ L304/64, as later amended <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0083> accessed 16 November 2022.

Article 3(3)(l) of the Consumer Rights Directive reads as follows: 'This Directive shall not apply to contracts: … (l) concluded by means of automatic vending machines or automated commercial premises'. The exception, however, does not refer to what is achieved with a Smart Contract, it being a self-executing computer programme, but refers to instant contracting through a device such as vending or parking ticket machines. This is confirmed by the Guidance Document on the Consumer Rights Directive, which provides the following example: 'This exception would apply to contracts concluded on automated commercial premises such as: Automated gas stations without the physical presence of the trader's representative for the conclusion of the contract.'[43]

The main question regarding the legal status, if any, of Smart Contracts is whether a Smart Contract can, as such (so without an already existing, underlying and preceding legally binding relationship) create a legally binding contract.

Smart legal contract: a basic European framework for contract formation can be found in the Draft Common Frame of Reference (DCFR).[44] The Reporters, therefore, took the DCFR as their overall accepted starting point for answering the question of whether a Smart Contract can be a legally binding contract. The Reporters also took as their starting point that both subjects involved (natural and legal persons) and the object (what is agreed upon?) must be clear and that an automated process by itself, without creating clarity regarding subjects and object, cannot produce legally binding acts. The answer to the question above concerning the legal status of a Smart Contract might be different depending on whether a consumer (B2C, G2C) or a professional party (B2B, B2G or G2G) is involved. The position of a consumer, entitled to pre-contractual information and post-contractual service, given the consumer's unequal bargaining strength against a professional party, is different from businesses negotiating at arm's length. It is beyond any doubt that consumer protection is needed more, when a contract formation takes place with the use of algorithms, which, from a consumer's viewpoint, create a 'black box', making it impossible to fully understand the technical side of the transaction. Consumer protection

---

43 DG Justice Guidance Document concerning Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (<https://ec.europa.eu/info/sites/default/files/crd_guidance_en_0_updated_0.pdf> accessed 16 November 2022) 10. The 'Study on Blockchains Legal, Governance and Interoperability Aspects' (SMART 2018/0038) (2020) seems to follow a different approach. See page 119 of the report, although the study does not provide any affirmative arguments. See also A Savelyev, *Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law* (14 December 2016). Higher School of Economics Research Paper No WP BRP 71/LAW/2016, Available at SSRN: <https://ssrn.com/abstract=2885241> accessed 16 November 2022 or <http://dx.doi.org/10.2139/ssrn.2885241> accessed 16 November 2022. Savelyev writes on page 9: 'Old-school vending machines automate performance only of one party, requiring at least some personal involvement on the other side (eg coin insertion or application of a banking card). When both parties' performance can be fully automated it creates a new quality of the contract, even triggering a question, whether there is still a contract in a legal sense and not some other kind of phenomena', while adding on page 17: 'In the latter case (ie a vending machine, text inserted by Reporters), although performance is automated, the seller – owner of the vending machine has the discretion regarding the performance of the contract: he may interfere in the process of functioning of such machine (eg by shutting it down) and thus, change the outcome of the deal. In Smart contract it is not possible for a party to it to change the outcome by shutting down its computer – all the transactions continue to exist and be processed in cyberspace.'

44 Ch von Bar, E Clive and H Schulte Nölke (eds), *Principles, Definitions and Model Rules of European Private Law. Draft Common Frame of Reference (DCFR, Outline Edition)* (Sellier 2009), Articles II.-4:101ff and Ch von Bar and E Clive, *Principles, Definitions and Model Rules of European Private Law. Draft Common Frame of Reference (DCFR, Full edition)*, Vol I (Oxford University Press 2010) 125ff, discussing Book II DCFR on contracts and other juridical acts.

which takes the specific algorithmic nature of a transaction into account can be secured in two ways: either by denying that a contractual relationship as such has come into existence, given that algorithms are as such neither readable nor understandable except by software developers and computer programmers, or by accepting that while a contract was concluded, the consumer is still entitled to protection, for example, a right to annul a clause or a right of withdrawal. The form of such right to annul or right to withdraw will, however, require adaptation given the technological environment in which this right must be made effective, compared to a right to annul or right to withdraw regarding contracts concluded through more traditional means, such as in writing. In both approaches, existing EU consumer law must be held against the light of how a Smart Contract functions. At the same time, it should not matter for the binding nature of a contract whether or not an e-commerce transaction takes place online, using Smart Contracts. The Smart Contract is the back side of the transaction and it is not questioned that a contract can be concluded using software, such as buying goods from a web shop online or by exchanging e-mails. Analysing the various technical stages of a Smart Contract (source code, bytecode, blockchain) when a decision has to be made as to legal consequences of what happens online was considered unnecessary. The question whether the law should focus on the formation process (eg is there an intention to create binding legal relations?) as such, or rather on the fact that source code, and certainly bytecode, cannot be read and understood by human beings, particularly not a consumer, can, of course, be asked. However, this problem is not new and is not specific to the use of Smart Contracts. It has generally been accepted that e-commerce transactions are valid.[45]

It is evident, for example when analysing the decision of the Singapore Court of Appeal regarding trade *via* a virtual currency exchange platform (*Quoine Pte Ltd v B2C2 Ltd*, [2020] SGCA(I) 02), that considerable uncertainty exists here.[46] However, the United Kingdom Jurisdiction Taskforce in its 2019 report entitled 'Legal Statement on Crypto Assets and Smart Contracts' already contained the following:[47]

> 'There is no reason why the normal rules should not apply just because a potential contract is a smart contract. It follows that the question of whether, and under what circumstances, a smart contract is capable of giving rise to binding legal obligations turns on the question of whether, and under what circumstances, parties engaged in smart contracting are capable of reaching objective agreement as to terms, of intending to create a legally binding relationship, and of satisfying the requirement of consideration.'

The views by the UK Jurisdiction Taskforce have, as recently as November 2021, been confirmed in a report by the English Law Commission on 'Smart Legal Contracts'.[48] As the report states:[49]

---

[45] The Study on Blockchains Legal, Governance and Interoperability Aspects (SMART 2018/0038) (2020) seems to follow a different approach. See page 119.

[46] See <https://www.sicc.gov.sg/docs/default-source/modules-document/judgments/quoine-pte-ltd-v-b2c2-ltd.pdf> accessed 16 November 2022.

[47] UK Jurisdiction Taskforce, 'Legal statement on Crypto Assets and Smart Contracts' (2019) 32, <https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf> accessed 16 November 2022.

[48] Law Commission, 'Smart Legal Contracts' (Law Com No 401) (HM Stationery Office 2021) 39ff.

[49] 'Smart Legal Contracts' 73.

> 'Given our conclusion that smart legal contracts can satisfy the requirements for a contract, a legislative statement that smart contracts are capable of being legally enforced (or to confirm that a contract is not unenforceable merely because it is a smart legal contract) seems unnecessary. In the absence of a real need for legislation, we do not think it would be justified.'

The UK Jurisdiction Taskforce also published a report on Digital Dispute Resolution Rules for arbitrations of digital disputes, facilitating arbitration in a blockchain and Smart Contract based environment.[50] In Rule 3 on incorporation, the report reads: 'These rules may be incorporated into a contract, digital asset or digital asset system by including the text (which may be in electronic or encoded form).' Again expressing that (computer) code can create legally binding relations. The approach is rather pragmatic, but is argued to be in line with practical needs, while at the same protecting the interests of consumers.[51] A report by the EU's Blockchain Observatory and Forum on 'Legal and Regulatory Framework of Blockchains and Smart Contracts', which discusses various aspects of Smart Contracts in light of existing contract law, does not reject *a priori* that Smart Contracts can be legally binding either. Further from this report, it becomes clear that a pragmatic approach to the issue is needed, as it would create grave uncertainty if blockchains and Smart Contracts functioned in a legal vacuum.[52] The same approach can be found in the 'Study on Blockchains Legal, Governance and Interoperability Aspects', prepared for the European Commission.[53]

We therefore take the position that the triggering of transactions, or of transaction elements, performed on a blockchain may amount to an offer, acceptance or any other contractual declaration where, depending on the specific nature of the Smart Contract, such triggering can reasonably be understood as a declaration of will and is attributable to the relevant party.

Principle 6 – Effectiveness of an On-Chain Declaration of Will

a) The point in time at which a contractual declaration as mentioned in Principle 5 becomes effective should be contractually agreed upon between the parties.

b) In the absence of such agreement between the parties, an on-chain declaration of intent may only trigger legal consequences if: (i) the recipient has actually received it; or (ii) the TRANSACTIONS are securely stored in the BLOCKCHAIN (ie cannot vanish in an orphan block).

---

50 <https://resources.lawtechuk.io/files/2.%20UKJT%20Digital%20Disupte%20Rules.pdf> accessed 16 November 2022.

51 See page 14 of the report where it is stated that a few exceptions exist as to not being able to submit a case to a court in case arbitration has been agreed: 'There are a few exceptions, such as where one party is a consumer not acting in the course of a business, and they are claiming a sum less than £5,000 from a business. In those circumstances, the consumer might be entitled to go to court instead if they choose to.'

52 EU 'Blockchain Observatory and Forum, Legal and Regulatory Framework of Blockchains and Smart Contracts' (2019) <www.blockchain4europe.eu/wp-content/uploads/2021/05/report_legal_v1.0.pdf> accessed 16 November 2022.

53 PYpma (et al), *Study on Blockchains Legal, Governance and Interoperability Aspects* (SMART 2018/0038) (2020). See particularly 117ff, discussing at 118ff consumer protection aspects.

Explanatory Notes

Triggering of transactions: the triggering of a transaction, particularly a Smart Contract, on a blockchain has three aspects: (1) the code which creates and, in fact, is the blockchain and that controls what is seen as a transaction, what that transaction may contain, when it is performed and what the outcome of that performance is; (2) the Smart Contract, which is also computer code functioning within the blockchain; and (3) what the parties off-chain intend to achieve with their contract. In the case of a public blockchain, the participants have no influence as such on the code that governs the blockchain. When the blockchain is private, the code can be programmed in such a way that what future contracting parties want as to how the blockchain functions is taken into account. This also applies to Smart Contracts, but to a lesser degree given that the Smart Contract functions within an already coded environment. Parties will have to take the coded environment into account if they want to use such environment as a tool for their contractual arrangements. They can, of course, try to code their pre-existing off-chain contract and mould the Smart Contract according to their wishes, but even then, especially in the case of a public blockchain, the enforcement of such encoded law would fully depend on the code governing the blockchain and any Smart Contracts which are already part of that code. Contracts in the more traditional sense of the word, where the contracting parties are known and which are not fully dependent on code, but could be a mixture of code and human writing, can more easily be created if the blockchain is private. In that case, the participants who can take part in the consensus process are restricted and known.

Transparency of intention to create legal relations: the intention to create legal relations, expressed in the process of offer and acceptance, must be transparent to both parties. Such transparency can be facilitated by ensuring that the offer and acceptance reach the other party (to avoid the occurrence of transactions of which the other party is unaware and did not signal any consent) or is accessible off-chain. This also solves any potential problems regarding the evidence of such transactions. If no explicit agreement between the parties involved exists, dispositive law applies. This raises the question of which law then governs, a question of private international law. This is still a very unclear and heavily debated area where the Principles only take a careful position. However, choice of law and choice of forum should be possible, allowing parties to decide for themselves which dispositive law applies, of course within the confines of public (international) law and public policy (*ordre public*). It should also be taken into account whether the parties are both businesses or whether one of the parties is a consumer. In the latter case, consumer protection must be safeguarded, irrespective of the fact that the transaction takes place in a coded environment (for further elaborations regarding consumer protection, see CONSUMER PRINCIPLES).

Public blockchains: when parties use a public blockchain, it is just as important as in the case of private blockchains that declarations of intent may only trigger legal consequences if: (i) the recipient has actually received them; or (ii) the transactions are either securely stored in the blockchain (ie cannot vanish in an orphan block) or securely stored off-chain. Within a coded environment, receiving a declaration of intent will mean having access to it, to which should be added having information about such access. A so-called orphan block is a block that is recognised by the blockchain (when two blocks are validly mined simultaneously), but was not accepted. How blockchains deal with orphan blocks may differ from blockchain to blockchain. In the absence of such agreement, dispositive law is applicable, whereby this can easily result in default of one party (eg in case declarations of intent vanish due to

orphan blocks). The difficulty here is that this will all depend on the code, which for the parties will be a given fact. Whenever a consumer is a party to such a contract, the position of the consumer must at least be equal to their position in an off-chain transaction. This could imply that, when such protection cannot be offered on-chain because of the code which governs the transactions, the rights of the consumer must be restored through an off-chain contract (for further elaborations regarding consumer protection, see CONSUMER PRINCIPLES).

Principle 7 – Formal and Substantive Validity

a) Rules concerning the formal and substantive validity of contracts under the applicable law apply to the conclusion of contracts on a BLOCKCHAIN; however, where the applicable law imposes formal requirements the purpose of which is also fulfilled by the use of BLOCKCHAIN technology, without the applicable law explicitly referring to BLOCKCHAIN technology, the formal requirements should be deemed to have been fulfilled.

b) A text form can generally be replaced with BLOCKCHAIN technology or a Smart Contract, whereas this might not apply to the condition of a written form if this implies a text document, either in writing on paper or in electronic format that is signed.

c) Formal requirements, such as the requirement that a contract must be in writing and signed, or needs to be drawn up in a particular format, such as an (authentic) deed, can only be fulfilled by a BLOCKCHAIN TRANSACTION or a SMART CONTRACT if the algorithmic representation of a written contract or deed equivalent to the off-chain use of such requirements:

(1) guarantees the same safeguards;

(2) accomplishes the purpose of such formal requirements; and

(3) regarding electronic signatures, fulfils the requirements of the electronic IDentification, Authentication and trust Services (eIDAS) or an equivalent regulatory framework.

Explanatory Notes

Functional equivalence and technological neutrality: the Principles are based on the need for functional equivalence and technological neutrality. These aspects, although closely related, are not the same. Functional equivalence means that solutions which are legally binding under already existing (off-chain) law should also be legally binding when new technology is being used. A question, for example, is whether a blockchain transaction, given its immutability and time stamp, could be seen as the functional equivalent of an authentic document. If the answer is in the affirmative, this does not immediately imply that civil servants or (civil law) notaries no longer have a role to play. Often, civil servants, (civil law) notaries or financial institutions are involved in cases where not only the authenticity of parties has to be established, but also other protective purposes are pursued (eg civil law notaries often have to fulfil certain legal obligations to explain and financial institutions have duties under their Know Your

Customer obligations). Also, with blockchain technology, there could be the problem that the private key to an identity could be stolen or hacked, whereas, in such cases, the authenticity of the holder of the private key to the identity would no longer be valid. Such risk of identity theft could be lower when civil law notaries are involved (although here, too, there is the risk of people forging IDs or similar). Blockchain technology can be a perfect tool to provide evidence and secure archiving, but the input still may have to be done by a person whose integrity and knowledge is beyond doubt. In other words: disintermediation may happen, but not necessarily so, even when blockchain technology is seen as functionally equivalent to an authentic document. A solution is technology neutral if it applies to and regulates relationships irrespective of the technology used. Blockchain technology as we know it today may (and perhaps will) develop further and a solution would then be technologically neutral if these new developments are also covered by existing law. Such law may then achieve functional equivalence, but as a result of technology neutral law.[54]

Text form and formal requirements: Principle 7(b) and (c), is again an expression of technological neutrality, functional equivalence and the fact that code should follow the law. The Principle differentiates between text form (with no signature attached) and written form (ie a text including the signature of someone). The distinction can be found in a more formalised manner, particularly in the German Civil Code, but may also be found, although perhaps more implicitly, in other legal systems.[55] The distinction is particularly relevant for consumers, as frequently their protection is safeguarded by a requirement that an agreement must be in writing, must be signed or even expressed in a solemn form such as a deed drawn up by a (civil law) notary or a deed prepared by a solicitor. The solemn form then implies the involvement of a legal expert, who can give advice to the parties. Text form can, generally speaking, be replaced with blockchain technology, whereas this might not apply to written form. Whenever a written form is required, it is now generally accepted that such a written form can be replaced by digital format. From this perspective, the Principle does not express anything new. More complicated questions arise, however, if not only a written form is required by a particular national legal system, but also a more solemn written form, such as, in the civil law tradition, an authentic (notarial) form and, in the common law tradition, the deed. Whether a blockchain transaction or a Smart Contract can replace these more solemn forms is a highly problematic and contentious question. However, if the blockchain transaction or the Smart Contract is performed under the responsibility of, for example, a (civil law) notary, public official or solicitor with the same precautions as exist if no coded environment were used, the rights of private parties will be sufficiently secure. In such a case, it can be said that equivalent to the off-chain use of such requirements, the same safeguards are guaranteed and the purpose of such formal requirements are being accomplished. Whenever electronic signatures are used, their validity has already been recognised as being sufficiently secure within, for example, the regulatory framework of the Regulation on electronic identification and trust services for electronic transactions in

---

54 Cf in this respect, A Veerpalu, 'Functional Equivalence: An Exploration Through Shortcomings to Solutions' (2019) Baltic Journal of Law & Politics 134ff.

55 See German Civil Code § 126 (written form), § 126a (electronic form) and § 126b (text form). The latter Section reads as follows: 'If text form is prescribed by statute, a readable declaration, in which the person making the declaration is named, must be made on a durable medium. A durable medium is any medium that 1. enables the recipient to retain or store a declaration included on the medium that is addressed to him personally such that it is accessible to him for a period of time adequate to its purpose, and 2. that allows the unchanged reproduction of such declaration.'

the internal market (eIDAS Regulation).[56] This principle fully recognises the legal effect of electronic signatures as stated in Article 25 of the eIDAS Regulation.[57] However, if such safeguards do not exist, the purpose of any off-chain formal requirements is not being accomplished or e-signatures are not secured as required by the eIDAS Regulation, blockchain transactions and Smart Contracts cannot fulfil that role.

Principle 8 – Language

a) Contracts between businesses and between private parties can be concluded on-chain; the parties can also agree that the contractual language is a programming language.

b) For Business to Consumer contracts, Principle 15 of the CONSUMER PRINCIPLES applies.

Explanatory Notes

Principle 8 builds on Principle 5, but is aimed at transactions between businesses as well as transactions between two private people (eg two consumers).

Natural and programming language: as an expression of private autonomy, the choice of the contractual language is free, as long as there are no special legal regulations to the contrary.[58] It is generally accepted that, particularly in a commercial setting, a contract may be concluded in a language other than the parties' native language, ie a foreign language.[59]

As it is accepted that a foreign language can be agreed upon as a contractual language, this must also apply to a (higher level) programming language, such as Solidity on the Ethereum blockchain – especially in a technologically open society. It can ultimately make no difference whether the parties agree '*ownership passes upon full payment*' or '*if ($AmountReceived >= $Price) {§OwnerDB[§AssetID] =$BuyerID;}*'.[60]

---

56 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/73. The European Commission proposed several changes to the eIDAS Regulation, introducing an 'e-wallet': Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, Brussels, 3.6.2021, COM(2021) 281 final.

57 Article 25 of the eIDAS regulation states: '1. An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures. 2. A qualified electronic signature shall have the equivalent legal effect of a handwritten signature. 3. A qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States.'

58 See for Austria, for example *Dullinger* in P Rummel, M Lukas, ABGB[4] § 883 No 1; see for Germany, for example *Emmerich* in MüKoBGB[7] (2016), § 311 No 1.

59 See, instead of many, for example C Kunkel, *Vertragsgestaltung* (2016) 107ff.

60 M Kaulartz, DSRITB 2016, 1029. Please note that the consequences of overpayment may be different in Civil Law compared to Common Law countries. From the perspective of the Common Law, in the case of accidental overpayment, the excess might be held on resulting trust for the payer, an approach which the Civil Law cannot follow as it does not have – generally speaking – a law on trust. This is, as such, unrelated to the use of code, but concerns the legal consequences of using code which, of course, may differ from legal tradition to legal tradition and even within a particular tradition from legal system to legal system.

Thus, it is submitted that programming language can be agreed upon as contractual language between businesses (of course, consumer protection rules fully apply; see CONSUMER PRINCIPLES).

Principle 9 – Off-Chain Prevails over On-Chain

Where a contract, or elements of a contract, concluded outside the BLOCKCHAIN is translated into CODE (such as with a view to implementing the contract, or parts thereof, by automated means), the terms of the contract concluded outside the BLOCKCHAIN prevail over any conditions coded on the BLOCKCHAIN, unless the parties have explicitly agreed otherwise.

Explanatory Notes

Conflict off-chain and on-chain: if a conflict arises between the text of an ordinary natural language version of a contract and the code version of such a contract, a question of contractual interpretation arises. A further conflict could arise whenever the bytecode version might diverge from the source code. This is an area where national approaches differ as to whether a more objective or a more subjective approach should be followed, or perhaps some middle ground should be found. The Principles do not take a position here, except for where the coded version of a contract diverts from the non-coded version or where there is a conflict between various levels of code. Given that the coded version will only be understood by software developers and computer programmers and is therefore far less intelligible than a traditional text, in such a situation the more intelligible version must prevail and that is the non-coded version. Following that line of reasoning, in case of a conflict between the source code and the bytecode version, the source code should prevail.

Enforcement problems: given the characteristics of blockchain technology (eg immutability), enforcement problems on-chain might arise (eg in the case of an unwinding of a contract and the need for a reverse transaction). How blockchain technology can (or should) adapt to ensure enforcement of rights on-chain has to be solved by technology experts, whereas, from a (merely) legal point of view, rights exist regardless of potential enforcement problems. In their recently published Global Code of Digital Enforcement, the International Union of Judicial Enforcement Officers formulated a set of Principles to deal with such enforcement issues in a coded environment.[61]

Principle 10 – Unwinding by Reverse Transaction

Where the applicable law provides for the unwinding of a TRANSACTION, such unwinding shall normally occur by a REVERSE TRANSACTION unless the BLOCKCHAIN at hand allows for the modification of blocks.

Explanatory Notes

[61] M Shmitz (ed), *Code mondial de l'exécution digitale/Global Code of Digital Enforcement* (Bruylant 2021). See also the contributions to D Walker (ed), *Cyberjustice, de nouvelles opportunités pour l'huissier de justice/Cyberjustice, New Opportunities for the Judicial Officer* (Bruylant 2021).

Frequently the only practical and effective solution in case a blockchain transaction is invalid or has to be terminated (for example, because of termination when the contract is not performed or as a consequence of annulment or withdrawal) will be the undoing of the transaction by a reverse transaction.[62] However, sometimes, when modification of blocks is possible, this might not be needed. It could also be that a particular legal system in certain situations of non-performance demands that, first of all, renegotiations take place to see if the existing problem can be solved by concluding a further agreement. Unwinding the original contract by way of a reverse transaction might then also no longer be needed. If both a reverse transaction and modification are either impossible, impracticable or ineffective, the only alternative left will be the claim for repayment of any funds already paid to the other party as well as, if applicable, payment of damages (eg for damage due to non-performance of the contractual obligation or damage caused because one party trusted that the contractual obligation would be validly fulfilled).

Principle 11 – On-Chain Dispute Resolution Agreements

Arbitration agreements implemented in the respective executing SMART CONTRACT (eg as a 'comment') may be agreed upon between businesses. Such arbitration agreements may also agree upon a dispute resolution ON-CHAIN.

Explanatory Notes

On-chain dispute resolution agreements: in commercial practice, arbitration, or other forms of dispute resolution, are common practice. Given that these Principles take as their starting point that Smart Contracts may result in legally binding agreements, it seems that arbitration or other dispute settlement agreements can also be concluded on-chain and executed on-chain. This is in line with a recent report by the UK Jurisdictional Taskforce on 'Digital Dispute Resolution Rules'.[63] In the foreword, the Taskforce summarises the aim of their rules as follows. The rules are:

> 'to be used for and incorporated into on-chain digital relationships and Smart Contracts. They are ground-breaking in that they allow for: Arbitral or expert dispute resolution in very short periods, Arbitrators to implement decisions directly on-chain using a private key, Optional anonymity of the parties.'

Given this development, a parallel approach is advocated for disputes to be decided within the EU.

It should, however, be noted that an arbitration agreement in a Smart Contract raises several complicated questions. It is impossible for a comment, as normally understood by programmers, to be incorporated into on-chain code. A comment included in off-chain source code is stripped out before compilations into bytecode, and it is bytecode which is executed on the blockchain, not the off-chain source code. A natural-language text string might be inserted into bytecode in such a way that visual inspection of the bytecode would reveal the arbitration clause. However, this seems far-fetched. It is not

[62] Unwinding could also be the outcome of a so-called "kill switch", a tool that allows a software process to stop instantly, for instance when the smart contract was initiated by accident, and reverses the process back to where it started.

[63] UK Jurisdiction Taskforce, Digital Dispute Resolution Rules (LawTech UK, 2021).

the usual programming practice – where it is technically possible without disrupting function – to embed non-functional text strings in bytecode. Furthermore, it is to be expected that a user would not normally inspect the bytecode in such a way as to have an opportunity to see and read such an embedded text string. Whether under these circumstances an arbitration agreement could be legally agreed upon, therefore, depends on the rules of a particular legal system as to the conclusion of legally binding agreements. This is, however, not different from answering the question whether, in a particular case, a Smart Contract as such can have a legally binding effect.

Problems might arise when a particular legal system demands that arbitration agreements are to be concluded 'in writing' and the question arises whether a Smart Contract or a transaction on a blockchain can be qualified as fulfilling the 'in writing' requirement.

On-chain dispute resolution (arbitration): the validity of a dispute resolution agreement (particularly arbitration) must be distinguished from the actual dispute resolution or arbitration process, resulting in a decision about the existing conflict. Such on-line dispute resolution or arbitration will be governed by rules of a more procedural nature. This Principle does not deal with these procedural aspects.

Consumer protection: the UK rules only offer very limited consumer protection. According to the accompanying text's further guidance, 'where one party is a consumer not acting in the course of a business, and they are claiming a sum less than £ 5,000 (approximately € 6,000) from a business … the consumer might be entitled to go to court instead if they choose to.'[64] This approach seems far too restricted, given the level of consumer protection which is offered in the EU and its Member States. The Principles, therefore, exclude any such agreement in case one of the parties is a consumer. At the same time, it should be noted that the Dispute Resolution Rules also deal with peer-to-peer or other voting by a community. According to the UK Rules, this is seen as an 'automatic dispute resolution process', and its outcome will be legally binding. The Principles do not take a position here, but a comparable approach within the EU might be considered, also given that the Principles assume that Smart Contracts may be legally binding and this might include any dispute resolution process within a particular blockchain community.

Principle 12 – Weaker Parties

WEAKER PARTIES shall be given the same or at least equal protection ON-CHAIN as they are entitled to OFF-CHAIN, from the perspective of both technological neutrality and functional equivalence, which must be adequate considering the algorithmic nature of a TRANSACTION.

Explanatory Notes

The Reporters as well as the Project Team wish to clearly state that on-chain transactions may not be used to undermine existing protection for weaker parties, such as consumers, tenants and employees.

64 Digital Dispute Resolution Rules, 14.

This Principle, therefore, states that such weaker parties are to be given protection that is in effect the same as they are given in a transaction that is off-chain. The protection should not only be functionally equivalent to off-chain protection, but it should also be such that any future technological changes – and developments in the area of IT which occur extremely fast – do not jeopardise the required level of safeguarding a weaker party's rights. This report does not deal with the position of weaker parties as such. However, as B2C transactions are a vital part of today's economy, the Reporters as well as the Project Team decided to dedicate Part II to CONSUMER PRINCIPLES. Still, next to consumers, for example, micro- as well as small- or medium-sized enterprises, tenants and employees could be confronted with transactions on a blockchain and the use of Smart Contracts, which might jeopardise their rights. A small entrepreneur is more often than not in the same unequal bargaining position and has the same information problems as an average consumer. A lease agreement could be completely on-chain and flexi-workers might be fully dependent upon Smart Contracts deciding about their temporary employment and working hours. Regarding these weaker parties, we recommend that further analysis be done about the consequences of algorithmic transactions and how these parties could be protected adequately by contract law, the law on leases and employment law. However, the Principles in Part II, which are dedicated to consumers, are not intended to cover any other weaker parties, although they might serve as a starting point for such further analysis and perhaps even become a source of inspiration for possible solutions.

2 PART II – Special Part on Smart Contracts and Consumer Protection

2.1 General Remarks – How to Define Who is a 'Consumer'

The Principles in Part I already provide a framework – although rather basic – for the protection of weaker parties, such as consumers, in cases where legally binding contracts are concluded with the use of transactions on a blockchain and more particularly Smart Contracts. Consumer protection is at the forefront of European law, as part of a broader framework to protect fundamental rights of European Union citizens. That framework also applies to the rights of European Union citizens, and hence consumers, in our rapidly developing digital economy, as expressed in the recently published European Declaration on Digital Rights and Principles for the Digital Decade.[65]

[65] European Declaration on Digital Rights and Principles for the Digital Decade, Brussels 26.1.2022, COM(2022) 28 final available at <https://ec.europa.eu/newsroom/dae/redirection/document/82703> accessed 16 November 2022. See also the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Establishing a European Declaration on Digital rights and principles for the Digital Decade (Brussels 26.1.2022, COM(2022) 27 final) and the Commission Staff Working Document, Report on the stakeholder consultation and engagement activities, Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Establishing a European Declaration on Digital rights and principles for the Digital Decade (Brussels 26.1.2022, SWD(2022) 14 final).

A preliminary question is how to define 'consumer' in a digital setting. The Principles are based on existing, and more traditional, concepts of consumer and B2C transactions and thus are founded on the existing European Union *acquis communautaire*. Even if the definition of consumer may vary from one Directive to the other, the most recent definitions all tend to be similar: 'any natural person who, in relation to contracts covered by this Directive, is acting for purposes which are outside that person's trade, business, craft, or profession' (Article 2[2] Directive 2019/771/EU). However, it should not be forgotten that, in an algorithmic environment, the aim and scope of the Principles might have to go beyond the classical concepts of consumer protection and might, for example, *also* apply to Peer-to-Peer (P2P) transactions. P2P may reveal different structures, such as a consumer (designated then as prosumer[66]) acting with another consumer. In this situation, the consumer is not so much being protected against a party with a stronger bargaining position, but rather against the technological tool (for example, a P2P transaction or platform) used, even though the counterparty may also very well be a consumer; or one party may be a SME and the counterparty a larger business.

Another aspect here is how to approach businesses which may pose as a consumer?[67] A reply could be that identifying the status of a contracting party (consumers versus businesses) is not only difficult in a blockchain context, but also in other, more traditional, contexts and therefore not a specific problem caused by an IT setting. At the same time, it must be admitted that it certainly is a problem in the platform economy.[68] The Modernisation Directive addresses that issue by inserting in Article 7(4) of the Unfair Commercial Practices Directive that a provider of an online market place must be informed by a third party whether that third party acts as a trader or non-trader.[69] Inspiration could also be drawn from the protection of consumers involved in investment transactions. The Markets in Financial Instruments Directive (MiFID II) qualifies clients according to their different levels of experience, knowledge and expertise and categorises them as either non-professional or retail clients, professional clients or eligible counterparties.[70] A professional client is 'a client who possesses the experience, knowledge and expertise to make its own investment decisions and properly assess the risks that it

66 The ECJ has denied the application of Directive 2005/29/EC on unfair commercial practices (UCPD) to a prosumer (P2P), ECJ Case, 04.10.2018, *Komisia za zashtita na potrebitelite v Evelina Kamenova* (C-105/17), ECLI:EU:C:2018:808, pt 35 and 40.

67 Cf G Howels, *Protecting Consumer Protection Values in the Fourth Industrial Revolution*, Journal of Computer Policy (2020) 145ff. See also Commission Notice, Guidance on the Interpretation and Application of Directive 2011/83/EU of the European Parliament and of the Council on Consumer Rights (2021/C 525/01).

68 See V Mak, *Legal Pluralism in European Contract Law* (Oxford: Oxford University Press 2020), 112ff, discussing the category of 'prosumers' as being in a platform economy 'a consumer who produces goods and services (118/9).

69 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 ('Unfair Commercial Practices Directive') [2005] OJ L149/22 and Article 3 of Directive (EU) 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 [2019] OJ L328/7. See also Commission Notice, Guidance on the interpretation and application of Article 6a of Directive 98/6/EC of the European Parliament and of the Council on consumer protection in the indication of the prices of products offered to consumers (2021/C 526/02).

70 Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast) [2014] OJ L173/349 (MiFID II).

incurs.'[71] The protection level is the highest for retail clients, is intermediate for professional clients (such as investment firms) and the lowest for eligible counterparties (for example governments).

In these Principles, we primarily focus on consumers (thus non-professional or retail clients), more in line with the Proposal for Markets in Crypto-assets Regulation.[72] In Article 3(28) of this proposed Regulation, a consumer is defined, as can generally be found in the EU *acquis communautaire*, as meaning 'any natural person who is acting for purposes which are outside his trade, business, craft or profession'. It was considered to introduce new terminology here. Such an approach can be found in the revised Package Travel Directive, which introduces the new legal category of 'traveller', but that Directive, according to its considerations, after all, still aims to protect consumers.[73] It seems that internal consistency with the proposed Markets in Crypto-assets Regulation is, at least for the moment, the better workable approach.

However, although the primary focus of these Principles is on consumers, it should also be realised that SMEs, next to tenants and employees, might be in the same dependent position as a consumer. With regard to SMEs, this becomes very clear when looking at the recently presented proposal for a Data Act. The proposal in its Article 13 provides protection of these enterprises against unfair contractual terms in agreements between enterprises unilaterally imposing their own terms and conditions on their weaker business counterparts concerning the access to and use of data or the liability and remedies for the breach or the termination of data-related obligations.[74] Article 13 then follows a structure, well-known from consumer law, which, after first defining in an open-ended norm what 'unfair' means, makes unfairness more explicit by adding a black list and a grey list of unfair clauses. However, the Principles in Part II of this report only deal with consumers, as already referred to in the Explanatory Notes under

---

71 See Annex II of the MiFID II Directive.

72 Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593 final. See also the recently introduced US Senate Bill to provide for responsible financial innovation and to bring digital assets within the regulatory perimeter ('Lummis-Gillibrand Responsible Financial Innovation Act'), 117th Cong. (2022) <http://www.congress.gov/> accessed 16 November 2022.

73 Directive (EU) 2015/2302 of the European Parliament and of the Council of 25 November 2015 on package travel and linked travel arrangements, amending Regulation (EC) No 2006/2004 and Directive 2011/83/EU of the European Parliament and of the Council and repealing Council Directive 90/314/EEC [2015] OJ L326/1. See recital 3 of the Directive in light of the text of the old package travel directive (Council Directive 90/314/EEC). Article 3 (6) defines traveller as follows: '"traveller" means any person who is seeking to conclude a contract, or is entitled to travel on the basis of a contract concluded, within the scope of this Directive'. Using such a type of definition in these Principles might make it more difficult to understand their ambit and main purpose, because – as can be seen in the Package Travel Directive – it would require a broad and specified definition as to who the counterparty of the consumer is which seems, given the approach in the proposal for a Markets in Crypto-assets Regulation, not a prerequisite for guidance as presented in these Principles.

74 Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final. For the definition of micro, small or medium-sized enterprises, Article 13 refers to Article 2 of the Annex to Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (notified under document number C(2003) 1422) (2003/361/EC). Article 2 of the Recommendation reads as follows: ' 1. The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million. 2. Within the SME category, a small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million. 3. Within the SME category, a microenterprise is defined as an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.'

Principle 12 on weaker parties. It has to be analysed whether the approach taken herein could also be applied to weaker parties in general.

2.1.1 Existing Approaches to Consumer Protection Applied to Smart Contracts

To clarify and underline what consumer protection means, several aspects of consumer transactions should be considered. Consumers are entitled to pre-contractual information rights, sometimes a reflection period, during which no contract is concluded yet and performance may not begin, or a right of withdrawal from a concluded agreement without giving reasons, or a combination of both a period of reflection and a right of withdrawal; sometimes certain specific formal requirements need to be fulfilled.[75] The Principles focus on the more general aspects of consumer protection in situations where a Smart Contract is used. It should, however, always be borne in mind that consumer protection may require more specific and explicit regulation in certain particular areas, resulting in sectorial protection as an expression of, and supplementing, a more general overall protection. Sectorial protection may, for example, be needed when consumers conclude financial transactions.

2.2 Principles

(a) Consumer protection cannot be overridden by SMART CONTRACTS or any TRANSACTION on a BLOCKCHAIN.

(b) If a consumer TRANSACTION takes place using BLOCKCHAIN technology or a SMART CONTRACT, consumer protection on-chain must be at least equivalent to the protection which a consumer would have had if no such technology or SMART CONTRACT had been used.

(c) Irrespective of the legal nature and contractual structure of a platform, the use of BLOCKCHAIN technology or a SMART CONTRACT shall not deprive consumers of any rights they might have had if the platform had not been used.

(d) The immutability of a BLOCKCHAIN TRANSACTION or the automatic performance and execution of a SMART CONTRACT shall not deprive consumers of any right they would have had if an equivalent legally binding agreement had been concluded off-chain.

(e) Businesses using SMART CONTRACTS have to consider rights of weaker parties, such as consumers, before deploying SMART CONTRACTS and ensure that the rights of weaker parties can also be fulfilled on-chain (eg by way of reverse TRANSACTIONS or modifiable SMART CONTRACTS).

(f) Consumers in good faith relying on a previous TRANSACTION on-chain should be protected against off-chain terms between businesses in the sense that any dealings between them on-chain are not binding or not binding on the same conditions as coded into the SMART CONTRACT.

Principle 13 – Consumer Protection Prevails Over and Fully Governs Coded Transactions

Explanatory Notes

The Principles take as their basis functional equivalence between consumer protection off-chain and on-chain, whereby, given the nature of an off-chain transaction, perhaps even greater protection is needed on-chain than off-chain. Unlike in the proposal for a Data Act, which defines functional equivalence from a technical viewpoint, functional equivalence in this report is referred to as aimed at reaching a comparable level of consumer protection.[76] For a consumer, it should not matter whether they are concluding a contract off-chain, on-chain or mixed, either with or without a Smart Contract. For example, when shopping at a supermarket, it should be irrelevant whether the customer goes to a physical cashier, puts the goods on the conveyor belt to then be scanned and paid for or whether the customer goes to a self-service scan, scans the goods themselves and pays by bankcard without any assistance from a supermarket employee. It should not matter whether the transaction takes place with or without human intervention, whether or not in the form of a transaction on a blockchain and irrespective of whether a Smart Contract is used. The customer should always be in the same or an equivalent legal position.

The same applies when a consumer uses a platform to buy any goods or services. Platforms can be organised in various ways and, consequently, have varying legal structures. A platform could only intermediate between the consumer and possible sellers and providers, thus bringing the parties, who then conclude their contract outside the platform, together. It could also be that the platform itself concludes contracts separately with the consumer and the seller or provider and then realises the actual exchange of goods or services. Again, for a consumer (or should one say a 'user') it should not matter how the platform is organised, what its legal nature is, how the contractual structure is designed and whether any transactions happen to take place with the help of Smart Contracts on a blockchain. The consumer should have the same, or at least equivalent rights and the same level of protection, on-chain as off-chain. The Principles thus express that technological neutrality and functional equivalence are key aspects of consumer protection in a coded environment when compared to consumer protection in a more traditional setting. Of course, it does matter who the final parties to the (Smart) Contract are: a user and a platform or only users of the platform, without the platform itself being contractually involved, but, from the perspective of consumers rights, these should be just as effective as if the contract had been concluded outside the platform.

Principle 13(e) states that businesses using Smart Contracts have to consider rights of weaker parties, such as consumers, before deploying Smart Contracts. They must also ensure that the rights of weaker parties can be fulfilled on-chain as well (eg by way of reverse transactions or modifiable Smart Contracts). A 'modifiable' Smart Contract is one that can be recoded while preserving ITS address, state

[76] The proposal for a Data Act in its Article 2(14) defines for the purposes of that regulation functional equivalence as follows: '"functional equivalence" means the maintenance of a minimum level of functionality in the environment of a new data processing service after the switching process, to such an extent that, in response to an input action by the user on core elements of the service, the destination service will deliver the same output at the same performance and with the same level of security, operational resilience and quality of service as the originating service at the time of termination of the contract'.

and balance. Perhaps another term for 'modifiable' could have been used, but – in full understanding, of course, as to how this must be done in practice by computer programmers – it does express clearly that a Smart Contract, if for example it is not in conformity with the protection consumers are given under the Unfair Terms Directive, must be recoded, but in such a way that the rights and duties of the parties under the previous Smart Contract are not affected. The immutability of a Smart Contract's outcome does not mean that the legal relationship which, in whole or in part may be shaped by a Smart Contract, is also immutable. A 'follow-up' Smart Contract that would make a previous Smart Contract 'mute' can change that relationship or express what should have been the content of that relationship in the first place.

Principle 13 also makes clear that the law prevails over (computer) code. The argument that coding a particular legal solution is too complicated, or perhaps even impossible, is not acceptable from a legal viewpoint. The law on consumer protection is the outcome of a long process of balancing rights and duties between contracting parties, characterised by inequality of bargaining power, in order to counterbalance the weaker position of a consumer vis-à-vis businesses and professionals. This is why consumer contract law is frequently of a mandatory nature, aimed at protecting natural persons, acting outside the scope of economic (trade, business or professional) activity. The fact that consumer transactions are concluded in digital format cannot result in taking away rights from consumers which they would otherwise have had. On the contrary, a digital transaction is for a consumer even less transparent and controllable than consumer transactions already are, particularly when, as more often than not will be the case, general terms and conditions apply. The use of a digital format only exacerbates existing problems in consumer transactions, because the digital process will be a 'black box' for any consumer. The 'take it, or leave it' situation in which consumers often find themselves and which already makes them even more vulnerable as such to undue pressure, disinformation and mistake, worsens when contract formation, content, performance and execution are not even accessible in natural language anymore, but in computer code. This results in a clear and unambiguous need to ensure that there is indeed at least equivalent protection on-chain as off-chain. This explains why the Principles express the need for functional equivalence, technological neutrality and that (computer) code must follow the law. In addition, under (e), the Principle also makes clear that businesses should be aware of the weaker position of consumers as their counterparties. They must consider the rights of structurally weaker parties before deploying Smart Contracts and ensure that their rights can also be fulfilled on-chain (eg by way of reverse transactions or upgradeable Smart Contracts). Non-compliance with such a duty could be a factor when deciding whether a contractual term is of an unfair character and falls under the ambit of the protection which the Unfair Terms Directive provides consumers with.[77]

Principle 13(f) deals with rather complex problems created when taking into account any third party effects, and particularly proprietary aspects, of contracts, and consequently also of Smart Contracts. Generally speaking, in certain legal systems, the conclusion of a contract may not have any proprietary effect, but in others that could be very different. If a (Smart) Contract of sale has proprietary effect, what is then the position of a third party if the parties to the Smart Contract conclude an off-chain

[77] Council Directive 93/13/EEC on unfair terms in consumer contracts [1993] OJ L95/29. Cf Article 4 (1): 'Without prejudice to Article 7, the unfairness of a contractual term shall be assessed, taking into account the nature of the goods or services for which the contract was concluded and by referring, at the time of conclusion of the contract, to all the circumstances attending the conclusion of the contract and to all the other terms of the contract or of another contract on which it is dependent.'

agreement declaring the Smart Contract as non-binding between them? Even if in a particular legal system contracts do not have any proprietary effect, still the question may arise whether a Smart Contract, as executed on a blockchain, could be seen as the delivery of what was promised. If so, even in legal systems which make a sharp distinction between contract and property, the position of third parties becomes relevant. We therefore include a Principle which protects third parties in good faith, when relying on the execution of a Smart Contract. Such reliance does not necessarily have to be of a strict proprietary nature, as it could also be more contractual. In certain legal systems, protection is given to a third party in good faith, relying on a contract which is known to that party, against a so-called *contre-lettre*: a contract which states, between the parties to a contract, that the latter does not express their real intentions. In an algorithmic environment, one can think of a declaration off-chain, unknown to a third party, stating that what is being concluded and performed on-chain will not be binding. A third party, relying in good faith on what happens on-chain, would not be aware of such a *contre-lettre* and should, therefore, be protected against the negative aspects of such an agreement. These problems are too complex to be dealt with in these Principles. However, Principle 13(f) does solve one specific problem from the perspective of a consumer, who, in good faith, relies on a previous transaction on-chain. Such a consumer should be protected against off-chain terms between parties to a Smart Contract to the extent that any dealings on-chain are not binding between them or not binding on the same conditions as coded into that Smart Contract. Examples are a B2B Smart Contract of sale in a jurisdiction where the sale transfers ownership or in which a producer gives guarantees about a product to a business selling that producer's products. If the parties to the Smart Contract would, off-chain and unbeknown to any third party, agree that they are not bound by any dealings on-chain, a consumer dealing with the business that sold the product may assume that the business owns the product and will pass on the same guarantees as were given to the consumer's counter party.

Principle 14 – Private International Law and Consumer Transactions

Choice of law and choice of forum clauses contained in SMART CONTRACTS used by a business in its dealings with a consumer are not to be given legal effect if a choice of law clause violates the rights of a consumer regarding the otherwise applicable law or the choice of forum clause violates the right to sue or be sued before the courts of their country of habitual residence or domicile.

Explanatory Notes

Given the difficulty in determining the applicable law to a transaction on a public blockchain, and considering that choice of law and choice of forum clauses are widely accepted as binding in the context of B2B transactions, the Principles accept (Principle 4) the validity of such clauses on-chain also. Of course, the binding effect of such clauses in B2B transactions is not without limitations and may, for example, be limited when violating public policy (*ordre public*) and cannot be decisive as to the proprietary effects of a transaction. The latter is generally governed by the *lex rei sitae* principle, but it should be borne in mind that precisely this principle does not have the same value on-chain as off-chain. On-chain *a situs* could be chosen (so-called 'elective *situs'*) which is then coded into the Smart Contracts as the applicable law, also regarding the proprietary aspects of the transaction. Such algorithms, however, would most likely only be binding within the blockchain environment and the problem remains what the impact will be outside that environment. This is a question on which these Principles do not take a position. The same applies regarding the impact of any obligatorily binding *lex registrationis*, such as requirements concerning registration of rights in an immovable property register.

A choice of law and choice of forum clause may also not be held valid in case a weaker party is entitled to protection under the law of their domicile, both with regard to the applicable law and the competent court (Principle 4(d)). An on-chain choice of law and/or choice of forum clause may, for that reason, be considered invalid (especially in the context of a B2C transaction). See in this respect, Article 6 of the Rome I Regulation and Article 17ff of the Brussels I Regulation, giving special protection to consumers.[78]

Internationally, the Canadian Supreme Court case of *Douez v Facebook* has drawn considerable attention, because of its far-reaching impact.[79] In its decision, the court stressed that such clauses should be evaluated differently in consumer settings, especially when contracts are concluded with social media, compared to commercial settings where the parties have a more or less equal bargaining power when negotiating at arm's length.

Principle 15 – Language and Consumer Transactions

> Agreements regarding the use of programming language cannot be concluded between businesses and consumers. SMART CONTRACTS used for consumers always have to be translated into NATURAL LANGUAGE.

Explanatory Notes

In addition to Principle 8, Principle 15 is an explicit rule for consumer contracts. Given that smart contracts are in coded language, Principle 8 states that contracts between businesses can be concluded on-chain; parties can also agree that the contractual language is a programming language (such as Solidity on Ethereum). However, such agreements cannot be concluded between businesses and consumers. Smart Contracts used for consumers always have to be made available as a translation (and explanation) into natural language so the consumer can read and understand what their rights and duties are.[80]

However, also in the case of consumers, a contract can be legally concluded by using a Smart Contract. It should not matter, as a result of the approach that the Principles seek functional equivalence, whether,

---

78 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L177/6 and Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2012] OJ L351/1.

79 <https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16700/index.do> accessed 16 November 2022.

80 In this context it can be mentioned that the Austrian Supreme Court recently decided that it is generally permissible to agree on a foreign language as the contract language between entrepreneurs and weaker parties. However, this requires an explicit reference, whereby the Austrian Supreme Court applied a very strict standard, stating that, in the event that the negotiating language is, for example, German, it would usually be grossly disadvantageous if the general terms and conditions were suddenly in a foreign language, despite the explicit reference. See OGH 22.12.2020, 4 Ob 213/20g. From the perspective of using a programming language instead of a natural language, this implies that, since Smart Contract code cannot usually be understood by consumers, an explicit reference to the fact that this code should apply will not be sufficient in consumer transactions. A consumer's counterparty (trader, business, professional) must take further steps to ensure that a consumer understands what they are agreeing to. The Principles offer some basic guidelines, such as in Principle 15.

at the backend of a web shop, more traditional software is used or a new technology such as a Smart Contract. Arguing that a consumer cannot understand computer code and therefore no legally binding agreement can come into existence would imply that e-commerce transactions as such are, as a matter of principle, not legally binding. This is a view that is both not generally accepted and unworkable in practice.

However, that consumers must know what they agree to and how algorithms govern their relationship with a business is not only true in cases where Artificial Intelligence is used, but each time that contract formation takes place with the use of software and more particularly Smart Contracts.[81] Consumer protection can then be given in two (cumulative) ways. This can be done through an abstract test by imposing a duty to audit the Smart Contract before it is used, so it is certified that, for example, the Smart Contract does not violate any fundamental human right, leading to nullity of the contract (cf for example, Article II-7:301 DCFR on contracts infringing fundamental principles).[82] Added to this can be a more concrete test, as can be found, for example, in the Directive on Unfair Contract Terms.[83] Article 5 of this Directive states, eg, that in 'the case of contracts where all or certain terms offered to the consumer are in writing, these terms must always be drafted in plain, intelligible language. Where there is doubt about the meaning of a term, the interpretation most favourable to the consumer shall prevail.' Computer code is a form of writing and must, therefore, be made available in plain, for the CONSUMER readable and understandable, natural language.

81 For individual protection against the use of Artificial Intelligence, see the European Commission's approach in its 2030 Digital Compass, 'The European Way for the Digital Decade' (2021).

82 For such audits in the realm of Artificial Intelligence, see the draft EU Artificial Intelligence Act, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final.

83 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, [1993] OJ L95/29.

Principle 16 – Consumer Information Rights

(a) CONSUMERS shall always have the same or functionally equivalent rights to information towards their counterparts (including platform operators or similar service providers) as they would have had if no TRANSACTION on a BLOCKCHAIN or SMART CONTRACT had been performed.
(b) This applies in particular to any pre-contractual information, but also to post-contractual information, such as part of a product recall, which a seller of goods or a supplier of services must give when the contract is not concluded using BLOCKCHAIN technology or a SMART CONTRACT.
(c) Such information must always be available off-chain, in natural, plain, intelligible and for the CONSUMER understandable language.
(d) CONSUMERS are, in advance, entitled to a translation and explanation of SMART CONTRACTS (both regarding procedure and substance) in natural, plain, intelligible and for the CONSUMER understandable language, updated whenever the SMART CONTRACT is updated, which must also be made available on a durable medium and publicly available on the user's website. If such translation and explanation are not made available, no legally binding agreement results from the SMART CONTRACT, or, in the case of an update, the agreement can be terminated.
(e) If the explanation deviates from the terms and conditions which apply once the contract has been concluded, the information contained in the explanation prevails or, if the deviation concerns essential characteristics of the contract, may result in the contract being avoided.

Explanatory Notes

Principle 16 is a further elaboration of Principle 13 and other Principles, as drafted earlier, aimed at preserving technological neutrality and functional equivalence, focussing on information duties. The duty to provide information may not only rest on a specific contractual counterparty, but could also rest on intermediary service providers, such as a platform operator and a wallet service provider. As the Principles' main goal is to reach functional equivalence regarding consumer contracts on-chain and off-chain, the addressee of any information duties should, first of all, be the specific contractual counterparty, such as a seller of goods or digital assets. However, in the contracting process, intermediary service providers (platform operators and wallet service providers) may play an important role. Such intermediary service providers may for a consumer also be a contractual counterparty, but could also very well be a provider of mere services used in the contracting process between the

consumer and a seller. These Principles apply primarily to any information duties which may rest on intermediary service providers with whom a contractual relationship exists. However, as stated in Principle 13, any protection to which a consumer is entitled against unfair commercial practices should also apply whenever Smart Contracts are used. Overall, the *acquis communautaire*, such as the Consumer Rights Directive and future EU law, such as the Digital Services Act, will apply as to the content and addressee of any information duties.

Duties to inform a customer before a contract is concluded are most important, but information while the contract is being performed (for example, about updates or product defects which were discovered) and even after performance as part of after-sales services or a product recall can also be of relevance.[84] The information must always be available on a durable medium in natural language to allow any consumer to read and understand what the information contains. The requirement of a durable medium can already be found in the E-Commerce Directive of 2000, stating in Article 10(3): 'Contract terms and general conditions provided to the recipient must be made available in a way that allows him to store and reproduce them.'[85] Generally, in EU consumer law, a requirement which must also be fulfilled is that the information must be in plain and intelligible language. This can, for example, be found in Article 8(1) of the Consumer Rights Directive. Hiding information behind technical language must be discouraged.

Principle 16 is also a further elaboration and clarification of Principle 8 by demanding that consumers are entitled not only to a translation, but also to an explanation of Smart Contracts in natural, plain, intelligible language that is understandable to them. The sanction is comparable to what we can already find in consumer law regarding unfair terms when these are not made available to the consumer: the consumer can withdraw from the contract. Another example can be found in the *acquis communautaire* which protects consumers when involved in transactions regarding packaged retail and insurance-based investment products (PRIIPS) by demanding that a Key Information Document (KID) is issued which contains basic pre-contractual information and which should be clearly distinguishable and separate from any marketing communications.[86] As Smart Contracts, given their algorithmic nature, will most likely be used only in a setting of mass and standardised transactions, otherwise the time and effort of coding such contracts do not seem worthwhile, consumers are not only in need of a durable medium on which the contractual terms and conditions are stored (ie *ex post*, after the contract has been concluded), but also need to know in advance (*ex ante*, before the conclusion of a legally binding contract) what the Smart Contract implies. Publication in natural language on the user's website will then give a consumer the easiest access to information about what the Smart Contract implies. The sanction here is that, if such information is not given as indicated, the consumer can withdraw from the legally binding agreement or, in the case of a non-communicated update, can terminate the agreement. In the first situation, an alternative could be that no contact has been concluded. This raises the issue, known from earlier stages of consumer protection law, whether, if standard terms and conditions have

---

84 C Thun and J Diels, *Consumer Protection Technologies: An Investigation Into the Potentials of New Digital Technologies for Consumer Policy*, Journal of Consumer Policy (2020) 177ff.

85 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [2000] OJ L178/1.

86 See the Key Information Document (KID) as prescribed in Regulation (EU) No 1286/2014 of the European Parliament and of the Council of 26 November 2014 on key information documents for packaged retail and insurance-based investment products (PRIIPs) [2014] OJ L352/1.

not been communicated, a contract has nevertheless been concluded, but the consumer may withdraw from such a contract, or that no legally binding agreement has come into existence given the absence of any implicit acceptance of such terms and conditions even. The first approach allows a consumer the option to either accept being bound or decide to end the agreement. The second approach does not allow such an option, but provides the consumer with the most far-reaching protection. This Principle, therefore, follows the latter approach.[87]

Information about updates cannot be used to unilaterally change the content of the contract. Changes are only possible within the limits set by the existing *acquis communautaire* regarding consumer protection, such as the Unfair Terms Directive and the Digital Content Directive.[88]

Principle 16(e) deals with the situation where pre-contractual information deviates from the actual terms and conditions once the Smart Contract takes effect. The consequences could be twofold. Either the pre-contractual information becomes part of the legally binding agreement or, if the deviation concerns essential characteristics of the contract, the consumer may avoid the contract.

87 Cf Commission Notice, Guidance on the Interpretation and Application of Council Directive 93/13/EEC of 5 April 1993 on Unfair Contract Terms in Consumer Contracts, C(2019) 5325 final.

88 For references to the Unfair Terms Directive, see above and, for digital content, see Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1.

Principle 17 – Duty to Code Cooling-Off (Consumer Right of Reflection or Right of Withdrawal)

(a) Whenever CONSUMERS are given the right to a cooling-off period such right must be:
  (1) coded into the SMART CONTRACT, to further protect CONSUMERS;
  (2) conferred in such a way that any right which a CONSUMER has regarding a cooling-off period can be exercised ON-CHAIN as OFF-CHAIN; and
  (3) communicated to the CONSUMER.

(b) A period of reflection shall be coded in such a way that the SMART CONTRACT only begins to execute in conformity with the applicable right to such a period.

(c) The SMART CONTRACT shall be programmed in such a way that when a CONSUMER exercises their right of withdrawal, the exercise of such right by itself results in a REVERSE TRANSACTION, taking into consideration the nature of the performance. If the nature of the performance prevents a REVERSE TRANSACTION, the CONSUMER may be entitled to a monetary claim representing the value of the TRANSACTION.

(d) The SMART CONTRACT shall be programmed in such a way that the CONSUMER is informed:
  (1) that the REVERSE TRANSACTION has taken place; and
  (2) that certain other rights, but also duties, might exist following the withdrawal.

(e) Coding a cooling-off period or a REVERSE TRANSACTION following the exercise of the right to withdrawal as part of the SMART CONTRACT will not be necessary if a CONSUMER would not be entitled to such a right, given, for example, the nature of the good, product or service.

Explanatory Notes

Principle 17 expresses another underlying policy choice on which these Principles are based. The phrase 'code is law' has become notorious. However, the law, as the result of balancing interests, cannot be discarded by computer programming, arguing that the software does not allow such balancing in a concrete case. The approach must be the reverse: the law should be programmed into the code and if such programming is not possible, at least the consequences of this should not rest on the shoulders of the structurally weaker parties, particularly consumers. This Principle, therefore, takes as its starting point that whenever and wherever a Smart Contract can be coded such that it safeguards and implements existing consumer protection law, the contract must be coded to reach that goal. This is in line with the development towards 'platform design duties', which can be seen in the area of regulating the platform economy. Such duties oblige a platform operator to structure the platform such that it becomes apparent, for example, whether a participant can be qualified as a business or as a consumer.[89]

Principle 17 introduces a duty to code a consumer's right to a cooling-off period into the Smart Contract. The aim is to strengthen an already existing consumer protection right. Given the fundamental nature of

[89] Cf Ch Busch, *Self-Regulation and Regulatory Intermediation in the Platform Economy*, in: M C Gamito and H-W Micklitz (eds), *The Role of the EU in Transnational Legal Ordering: Standards, Contracts and Codes* (Edward Elgar, 2020) 115ff, 124 referring to O Sylvain, *Intermediary Design Duties*, Connecticut Law Review (2018) 203ff.

a cooling-off period, information about this right is of utmost importance for a consumer. When the contractual process is fully automated, such process must include, as part of coding the law into the Smart Contract, notifying consumers of their rights. This can be done, for example, by a notice on a computer screen or by sending the consumer an e-mail with that information.

The term 'cooling-off' period is not always very precise in what it actually means. Under EU consumer law, it can mean a period of reflection, during which there might be a binding offer, but the consumer has a right to consider acceptance and hence no legally binding contract yet exists, or a period following the conclusion of a legally binding contract during which the consumer has the right to withdraw from that contract. Reference can be made to a report by the European Commission to the European Parliament and the Council on the review of Directive 2014/17/EU of the European Parliament and of the Council on credit agreements for consumers relating to residential immovable property.[90] The report states on p 5:

> 'Following transposition of the Directive, Member State legislation now gives consumers a period of reflection, withdrawal or both, which they did not always have before. Most Member States opted to grant a period of reflection rather than a period of withdrawal. Despite this, the proportion of consumers who felt that they are given enough time to reflect has fallen (compared to before the Directive was implemented).'

It should be noted, however, that the terms 'cooling-off period' and 'right of withdrawal' are sometimes used interchangeably and sometimes not.[91]

In case of a reflection period, where the consumer is not yet bound by a legally enforceable agreement, the Smart Contract must not start to run immediately. It can only be triggered by the consumer accepting the offer. In case of a right to withdraw, using that right should be made possible as part of the Smart Contract as well, and result in an automatic reverse transaction. If this is not possible because of the nature of the goods sold or services delivered, the reverse transaction should either take place later, but as quickly as possible, or result in a claim for reimbursement of the value. An intermediate solution between an immediate reverse transaction and a claim for reimbursement of the value might be to ensure a deposit in an escrow account. Such a deposit should, however, only be made for the

---

[90] The report can be accessed at <https://eur-lex.europa.eu/resource.html?uri=cellar:ba9380c3-b23d-11eb-8aca-01aa75ed71a1.0015.02/DOC_1&format=PDF> accessed 16 November 2022.

[91] See Article 14(6) of Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010 [2014] OJ L60/34, and recently Article 26(1) and (7) of the Proposal for a Directive of the European Parliament and of the Council on consumer credits, COM(2021) 347 final. Recital 23 of the first mentioned Directives states: '(23) It is necessary to regulate some additional areas in order to reflect the specificity of credits related to residential immovable property. Given the significance of the transaction it is necessary to ensure that consumers have sufficient time of at least seven days to consider the implications. Member States should have flexibility to provide this sufficient time either as a period of reflection before the credit agreement is concluded, a period of withdrawal after the conclusion of the credit agreement or a combination of the two. It is appropriate that Member States should have the flexibility to make the reflection period binding on the consumer for a period not exceeding 10 days but that in other cases consumers who wish to proceed during the reflection period are able to do so and that, in the interests of legal certainty in the context of property transactions, Member States should be able to provide that the reflection period or right of withdrawal should cease where the consumer undertakes any action which, under national law, results in the creation or transfer of a property right connected to or using funds obtained through the credit agreement or, where applicable, transfers the funds to a third party.'

period needed for a reverse transaction and may not be used to limit a consumer's right to either a reverse transaction, their entitlement to reimbursement of value or a claim for (supplementary) damages.

Currently, the Consumer Rights Directive differentiates between contracts for the sale of goods, on the one hand, and contracts for the supply of services or digital content or grid-bound supply of, for example, electricity, on the other.[92] Where it is not difficult to unwind a transaction, the Consumer Rights Directive currently does not provide for a moratorium. Principle 17 does not explicitly differentiate in the same manner according to the subject matter of the contract, but given the purpose of the Principle, ie that the consumer is given the same protection on-chain as off-chain, the relevant provisions of the Consumer Rights Directive might be applied by analogy.

Principle 17(a) and (d) contain the duty to code into the Smart Contract that the consumer is given information about their right regarding the cooling-off period, a reverse transaction triggered by the exercise of a right of withdrawal and further rights, but also duties, flowing from a withdrawal.[93]

Finally, Principle 17(e) contains an exception to the coding duties under Principle 17(a)–(d) whenever a consumer in an off-chain setting would not have been entitled to either a period of reflection or a right of withdrawal. See, for example, Article 16 of the Consumer Rights Directive, as recently revised by the Better Enforcement and Modernisation Directive.[94] If, generally speaking, consumers, after having been given clear and unambiguous information about their rights, would waive their rights under a period of reflection or a right of withdrawal, by giving express (ie not implicit) prior consent, there would also not have been any rights under a cooling-off period in an off-chain setting. Consequently, the consumer will then not be in a different situation when a Smart Contract is being used. The same applies in case a right of withdrawal exists if the nature of the good, product or service is such that, once performance took place, it cannot be undone. An example is the supply of digital content, see Article 16(m) of the Consumer Rights Directive.[95]

92 Cf Article 9 of the Consumer Rights Directive.

93 Cf Articles 13 and 14 Consumer Rights Directive.

94 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, [2011] OJ 2011 L304/64 and Directive (EU) 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, OJ 2019 L328/7.

95 Article 16(m) reads as follows: 'Member States shall not provide for the right of withdrawal set out in Articles 9 to 15 in respect of distance and off-premises contracts as regards the following: (…) (m) contracts for the supply of digital content which is not supplied on a tangible medium if the performance has begun and, if the contract places the consumer under an obligation to pay, where: (i) the consumer has provided prior express consent to begin the performance during the right of withdrawal period; (ii) the consumer has provided acknowledgement that he thereby loses his right of withdrawal; and (iii) the trader has provided confirmation in accordance with Article 7(2) or Article 8(7).'

(a) The protection of CONSUMERS against unfair terms shall be as effective ON-CHAIN as OFF-CHAIN.
(b) A standard term that any agreement can only be concluded in digital format (ie ON-CHAIN, using SMART CONTRACTS) is, as such, not an unfair term.
(c) CONSUMERS shall have the right to terminate a contract ON-CHAIN if it was concluded ON-CHAIN.
(d) The provisions of the Unfair Terms Directive, and the *acquis communautaire* which has been developed around this Directive, shall be equally applicable as to whether a term in a SMART CONTRACT is unfair and, if so, which legal consequences this may have. The legally binding agreement shall then not contain the unfair term. In case the unfair term is a self-enforceable part of a SMART CONTRACT, the CONSUMER is entitled to immediate redress by having the contract re-coded.
(e) Whenever a clause has been declared unfair in collective proceedings (such as under the Injunctions Directive or the Representative Actions Directive), there should be a duty on the relevant business to re-code all SMART CONTRACTS affected.

Principle 18 – Unfairness Control (Unfair Terms) in Consumer Transactions

Explanatory Notes

One of the central tenets of EU consumer law is the Unfair Terms Directive from 1993.[96] The Directive lays down the fundamental rules on protection of consumers against a contractual term which has not been individually negotiated and which shall be regarded as unfair if, contrary to the requirement of good faith, the term causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer (Article 3(1) Unfair Terms Directive). Such a clause shall, as provided for under national law, not be binding on the consumer (Article 6(1) Unfair Terms Directive). This Directive must be applicable irrespective of the format in which the consumer concludes legally binding agreements. The use of a digital format, and consequently of coded language, which a consumer can neither read nor understand, demands an even greater need for protection. Applying code already by itself implies a 'take it, or leave it' approach. Consumers are not only the structurally weaker party in their relations with a trader, business person or professional regarding the essential characteristics of any agreement (product, service, price, etc), and more particularly any pre-defined terms and conditions, but also concerning the algorithmic form of both the transaction and the conditions upon which it is concluded. The Directive provides, also in light of the *acquis communautaire* which has been developed around this centrepiece of European Union consumer law, a workable framework also when an agreement is concluded on-chain, while using Smart Contracts. Nevertheless, following Principle 7, it

[96] Already referred to above. See also Directive (EU) 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 [2019] OJ L328/7 and Commission notice, Guidance on the interpretation and application of Council Directive 93/13/EEC on unfair terms in consumer contracts (2019/C 323/04) [2019] OJ C323/4.

cannot be unfair as such if a term requires that a legally binding agreement can only be concluded in digital format (on-chain, using Smart Contracts). A clause like this could be part of the terms and conditions which are part of the offer and may, as a consequence once the offer has been accepted, also apply to any later changes to the contractual terms and conditions. The Principle builds upon Article 9(1) of the E-Commerce Directive, which provides that:

> 'Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means.'

In case such a term requiring conclusion in digital format is used, the consumer must also be given the right to terminate the contract on-chain and this should not be made unnecessarily difficult. If, for example, a subscription to a newspaper or magazine can be concluded on-chain, by means of the publisher or seller using a Smart Contract in the contracting process, it should not be required from the consumer that termination of the subscription can only be done by written notice sent by ordinary mail. Termination should then also be made possible by the same easy and fully automated process as when the subscription was agreed upon.

The structural imbalance, due to the unequal bargaining position of the consumer, the lower level of information available and lack of relevant knowledge, must be taken into account by allowing the consumer to declare an unfair term to be non-binding. The legal consequences will then be governed by the same legal framework as applies under the Unfair Terms Directive. This Principle, under (d) and (e), deals with the consequences of a term in a legally binding Smart Contract being unfair. First, the Principle states that if a term in a Smart Contract is unfair according to the Unfair Terms Directive, the provisions of this Directive (and of course pursuant to the *acquis communautaire* which has been developed by the courts based on this Directive) will be equally applicable. The legally binding agreement will then not contain the unfair term. Problems which may arise here must be solved by the applicable law in light of the *acquis communautaire* in this area.[97] If necessary, a (partial) reverse transaction may have to follow. Following Article 6(1) of the Unfair Terms Directive, the contract (ie the legally binding agreement) shall continue to bind the parties upon the remaining terms if it is capable of continuing in existence without the unfair terms. It should be understood that a term that is not binding in an algorithmic environment may have to be looked at from a very different perspective compared to if this problem arose in a more traditional setting. The protection which a consumer needs will have to take into account the digital nature of the unfair clause and the fact that it is embedded in a Smart, ie self-executing, Contract. Therefore, the Principle adds that, in case the unfair term is a self-enforceable part of a Smart Contract, the consumer is entitled to immediate redress by having the contract re-coded. Again, any problems arising as a consequence of this will have to be solved by the applicable law in light of the *acquis communautaire*. The same type of problem arises whenever a clause has been declared unfair in collective proceedings (such as under the Injunctions Directive or the Representative

[97] See M Loos and J Luzak, *Update the Unfair Contract Terms Directive for Digital Services*, Study requested by the JURI committee of the European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 676.006 (European Parliament: Brussels 2021) 13.

Actions Directive).[98] To give consumers an effective level of protection, there should be a duty on the relevant business to re-code all contracts affected. The question remains as to what the duty of a business is when it obtains a notice of the fact that a clause is most likely unfair, for example because it was declared unfair in proceedings against another business. However, this problem is not specific for Smart Contracts and raises procedural questions relating to the doctrine of *res iudicata*. Procedural questions are generally not within the scope of these Principles.

[98] Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests (Codified version) [2009] OJ L110/30, to be replaced by Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC [2020] OJ L409/1.