European Commission

Study on Blockchains

Legal, governance and interoperability aspects (SMART 2018/0038)

FINAL REPORT

A Study prepared for the European Commission DG Communications Networks, Content & Technology by:

Digital Single Market

This study was carried out for the European Commission by

Patricia Ypma
Esther Tenge
Peter McNally
Kaja Kaźmierska
Network of national legal experts

Dr. Michèle Finck

Professor Paul Foley
Alexander Gemmell
Selina Patel
Richard Potter
David Sutton

Rebecca Lynn Johnson
Yukitaka Nezu
Martin Schäffner

Internal identification

Contract number: LC-01180124
SMART 2018/0038

DISCLAIMER

By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

ISBN 978-92-76-16306-0
doi: 10.2759/4240

Luxembourg: Publications Office of the European Union, 2020

Table of Contents

Figures

Tables

Abstract

This report is the result of the 'Study on Blockchains: legal, governance and interoperability aspects (SMART 2018/0038)' (also referred to as: the 'Study') carried out by Spark Legal Network, Michèle Finck, Tech4i2 and Datarella for the Commission's Directorate-General for Communications Networks, Content and Technology, Directorate F: Digital Single Market, Unit F3: Digital Innovation and Blockchain. The overall objective of the Study is to provide evidence and support for policy approaches and concrete actions within the European blockchain initiative and to contribute to the building of an EU strategy in light of blockchain developments. The Study therefore analyses and assesses the legal framework in the EU with regard to blockchain technology and presents policy options where a need for adjustment or clarification is required. Additionally, the Study assesses what the impacts of blockchain and the proposed policy options could be on the economy and society with a view to considering future blockchain policy developments.

Abstrait

Ce rapport est le résultat de l'« Etude sur les Blockchains : aspects juridiques, de gouvernance et d'interopérabilité (SMART 2018/0038) », (ci-après dénommée l´« Etude ») réalisée par Spark Legal Network, Michèle Finck, Tech4i2 et Datarella pour la Direction Générale des Réseaux de Communication, du Contenu et de la Technologie de la Commission Européenne, Direction F : Marché Numérique Unique, Unité F3 : Innovation Numérique et Blockchain. L'objectif global de l'Etude est de fournir des preuves et un soutien aux approches politiques et aux actions concrètes dans le cadre de l'initiative européenne « Blockchain » et de contribuer à l'élaboration d'une stratégie de l'UE à la lumière de l'évolution de la blockchain. L'Etude analyse et évalue donc le cadre juridique de l'UE concernant la technologie blockchain et présente des options stratégiques lorsqu'un besoin d'ajustement ou de clarification est nécessaire. En outre, l'Etude évalue quels seraient les impacts de la blockchain et des options stratégiques proposées sur l'économie et la société, en vue d'examiner les potentiels développements politiques futurs de la blockchain.

Executive Summary

This document constitutes the Final Report for the 'Study on Blockchains: legal, governance and interoperability aspects (SMART 2018/0038)' (also referred to as: the 'Study') carried out by Spark Legal Network, Michèle Finck, Tech4i2 and Datarella (together also referred to as: the 'Consortium') for the Commission's Directorate-General for Communications Networks, Content and Technology, Directorate F: Digital Single Market, Unit F3: Digital Innovation and Blockchain.

Objectives and methodology

The overall objective of the Study is to provide evidence and support for policy approaches and concrete actions within the European blockchain initiative and to contribute to the building of an EU strategy in light of blockchain developments. The Study therefore analyses and assesses the legal framework in the EU with regard to blockchain technology and presents policy options where a need for adjustment or clarification is required. The Study also assesses what the impacts of blockchain and these policy options could be with a view to consider future blockchain policy developments.

Data collection

In order to meet the above-mentioned objectives, data was collected through both desk and field research. With regard to the desk research, the Consortium consulted all literature relevant to the Study in order to identify and appreciate the technical, economic and governance context applicable to blockchain technology and to gain insight into the legal issues regarding blockchain technology. Moreover, a team of national legal experts completed a legal research questionnaire, covering France, Germany, Italy, Spain, the UK (including Gibraltar), the United States, Switzerland and Singapore. The completed legal research questionnaires show in a comparable fashion how the national regulatory frameworks address key aspects relevant to blockchain and facilitate a better understanding of the relevant legal rules and regulations in these countries.

Additionally, the Consortium conducted field research via two types of interviews. The first set of interviews were conducted with key stakeholders in the field. The group of stakeholders consisted of (representatives of) industry and socio-economic organisations, venture capitalists and legal experts and / or law firms dealing with blockchain on a regular basis. The second type of interview was held with representatives of the national financial regulators. During these interviews, the views of the interviewees were sought on the regulation of utility token ICOs.

Setting out the technical, economic and governance context applicable to blockchain technology

In order to have an all-round picture of some of the most important aspects of blockchain technology – including where its opportunities and risks lie - the Consortium examined the technical, economic and governance context applicable to blockchain technology. In the first instance, this entailed looking into the technical context and setting out what blockchain technology constitutes and entails exactly, and what varieties of blockchain there are. Secondly, the topics of transaction capacities, environmental concerns, and cybersecurity were considered. Lastly, the Consortium investigated the issues of integration with legacy systems, interoperability and

standardisation, tokenisation as a means to provide incentives, and organisation and governance aspects.

Identifying the legal issues regarding blockchain technology

After setting out this context, a number of general legal issues in relation to blockchain technology were identified and considered. The first of these issues concerns the responsibility for legal compliance and liability. The second issue identified is that of the potential barriers in sectoral legislation that may prevent blockchains from unleashing their socio-economic potential in the EU, and the potential impact of DLT on data retention rules, such as those arising under the Anti Money-Laundering Directive. Thirdly, the protection of fundamental legal principles and mandatory rules is examined. DLT can also be used to infringe fundamental legal principles or mandatory rules (such as the prohibition of child abuse materials, drug trafficking or money laundering) and it can be difficult to remove related content from the database. The fourth legal issue identified is that of the tension between blockchain reality and legal reality. There may be situations for example where from a legal perspective, ownership changes, yet this is not reflected on-chain.

Additionally, the Consortium identified a number of legal issues with regard to smart contracts, starting with the application of contract law. Here, it is observed that contract law applies to smart contracts provided that these indeed qualify as legal contracts. One element to which particular attention is paid is that of smart contracts' cross-border dimensions. Next, the national legal requirements on the need for a written form of the contract are considered. Thirdly, the application of consumer law to smart contracts is discussed. Automated transactions characterised by high complexity can be problematic, as non-experts cannot grasp what the smart contract transposes at a technical level. However, smart contracts also present potential opportunities from a consumer protection perspective. Following this, the issue of smart contracts and pseudonymity is identified and examined. In this regard, pseudonymity presents advantages (such as from a data protection perspective) and disadvantages (such as from the Anti-Money Laundering (AML) standpoint) from a legal perspective. The fifth issue evaluated is that of smart contracts and jurisdiction. Blockchains are useful to coordinate actions between different actors, which can be located in various locations, raising questions of applicable law and jurisdiction. Following this, the issue of the capacity to contract and the protection of minors is assessed; if one does not know whether a party lacks capacity or a minor is involved, for example, then it is impossible to determine whether they have capacity to contract. The seventh area of examination is that of opacity. It deals with the questions of how parties without the necessary technical background can negotiate, draft and adjudicate smart contracts. Smart contract arbitration mechanisms and in particular the question of the compatibility between smart contract arbitration mechanisms and legal requirements regarding arbitration proceedings are also assessed. Finally, the Consortium looked at the potential impact of smart contracts on notarisation. Many have argued that DLT could facilitate the notarial profession's task due to its tamper-resistance and possibility of coordination through multiple parties. It is, however, sometimes feared that legal requirements around notarisation could prevent digital transactions from being concluded purely through digital means.

The legal issues in relation to utility tokens were set out as well. The lack of legal certainty as to how various existing legal frameworks ought to be applied to blockchain use-cases and regulatory fragmentation is covered in detail. Secondly, the application of consumer protection law as well as prospectus requirements to utility tokens are examined. Finally, trading on secondary markets is discussed. Some have highlighted that if there is a secondary market for tokens, there is a risk of market abuse (such as

insider dealing and market manipulation) and in relation to utility tokens there is also a risk that these are being purchased as a speculative investment (which could then turn them into a security on the secondary market).

Outlining the policy options

Subsequently, the Consortium outlined the various possible policy options available to the European Commission. More specifically, the wait-and-see and issuing of guidance approaches are discussed, as are the options of new supranational secondary legislation, the opt-in regime and regulatory sandboxes. Each policy option is introduced descriptively before moving on to outline their respective advantages and disadvantages.

Legal and socio-economic analysis

As part of the legal analysis, policy options were assessed and developed for the issues identified with regard to blockchain technology, smart contracts and utility tokens, with the aim to address a potential need for adjustment or clarification of the legal or policy framework and in order to enable the EU to continue to nurture a compliant and internationally competitive blockchain sector. In order to validate the results and the preliminary policy options, a stakeholder workshop was organised on 2 December 2019. Based on the feedback received at the workshop, the Consortium refined and finalised its findings.

Furthermore, the impact of blockchain technology on the economy and on society was assessed. This economic analysis considers how services will evolve and provides an overview of the impact of policy options on the economy and society.

The (results of the) legal and socio-economic analysis are set out in more detail below.

Assessment of policy options in light of the legal issues relating to blockchain technology

General legal issues pertaining to (the development of) blockchain

Firstly, with regard to the general legal issues that have emerged regarding blockchain technology, it was found that in terms of the *responsibility for legal compliance and liability,* challenges are not due to shortcomings of the respective legal frameworks but rather to the fact that blockchain systems and specific use cases thereof may not have been designed with a view to complying with legal requirements. As a result, the Consortium considers that no specific policy response is needed and recommends that the Commission adopt a wait-and-see approach. Furthermore, better technical and governance design could enhance compliance. Whereas this is not foremost a task for public authorities, the Commission could incentivise industry efforts to this effect. Lastly, stricter law enforcement by relevant national and supranational agencies would underline that compliance is not optional and create incentives for compliance for industry.

With regard to the issue of *potential barriers in sectoral legislation*, the Consortium found that ensuring compliance with AML legislation is essentially a governance question (for the actor using blockchain) as well as a question of the effective enforcement of existing regulations (from the public authority perspective) and therefore a specific policy response in relation to this legal issue is not required. It is suggested that the Commission adopt a wait-and-see approach. However, should the Commission wish to adopt a more active approach, it could proactively encourage industry that blockchain-

based AML systems are designed in order to ensure compliance with existing regulation from a technical perspective such as through research funding. Additionally, the adoption of standard terms and conditions or contracts could be used to coordinate compliance (e.g. model contracts ensuring that the related sharing of information between numerous actors for AML purposes is respected).

In relation to the matter of the *protection of fundamental legal principles and mandatory rules*, the research revealed that existing principles appear well-suited to addressing problems associated with the criminal use of this technology. There is thus no immediate need for a concrete policy action and the European Commission should adopt a wait-and-see approach.

The Consortium identified the *tension between blockchain reality and legal reality* as a technical design and human governance issue not unique to blockchains. The research therefore finds that there is no immediate need for policy action, and recommends the adoption of a wait-and-see approach in this context. Should the Commission already want to adopt a more proactive approach, it could encourage the development of technical and governance solutions that are aimed at aligning on-chain and off-chain information (such as guidance on best practices) and provide research funding for projects seeking to address such issues (which are also of broader relevance for the digital economy).

Smart contracts

In relation to smart contracts, the Study found that whereas smart contracts by no means always qualify as legal contracts, they can in cases where they meet the relevant definition of a valid contract in national legislation. Pursuant to the research findings, the issue of the *application of contract law* to smart contracts is not seen as a cause for concern by relevant stakeholders. As a result, no specific action needs to be taken at this stage, and the Commission could adopt a wait-and-see approach. Regarding the specific case of cross-border transactions, it may be that a contract valid in one jurisdiction is not valid in another, and there is some uncertainty surrounding the question of whether Article 3(1) of the Rome I Regulation applies to blockchain-based assets. Whereas this is a matter that would ultimately have to be clarified by the Court of Justice of the European Union or a revision of the Rome I Regulation, it may be beneficial if the Commission issue regulatory guidance on this matter in the meantime.

Secondly, the research revealed that the fact that requirements that *national contract law provisions require a written contract* which apply in some circumstances seem to operate in a technology-neutral manner to protect important policy objectives. What is more, in many scenarios these requirements can be fulfilled where the contract is in electronic form. It is thus recommended that the Commission adopt a wait-and-see approach.

Thirdly, as stakeholders did not flag specific legal issues arising in relation to the *application of consumer law to smart contracts*, the Commission could adopt a wait-and-see approach. Regarding the specific issue of the right to withdrawal under the Consumer Rights Directive, the Commission could engage a discussion on whether consumers' withdrawal rights create an undue burden on smart contracts as part of the next revision of this legal regime (in accordance with Recital 62 of the Consumer Rights Directive). In the interim, it could also choose to adopt regulatory guidance on how exactly consumer protection law applies to smart contracts.

Regarding *smart contracts and pseudonymity*, the Commission could encourage the adoption of standard contractual clauses related to the identification of the parties to a

contract. Beyond this, the Commission could also monitor this issue, and if considered appropriate, encourage the development of digital and/or SSI systems, such as for instance through research funding.

Concerning *smart contracts and jurisdiction*, existing supranational legislation such as the Brussels I and Rome I regimes appear well-suited to govern related issues so that the adoption of a wait-and-see approach seems well-suited in this domain.

With regard to the *capacity to contract and minors*, there does not appear to be an immediate need for regulatory intervention in the domain, favouring a wait-and-see approach. The Commission could, however, provide research funding for projects seeking to provide innovative solutions.

In relation to *opacity*, existing supranational secondary legislation already seems to contain mechanisms to address the disadvantages that opacity may generate for consumers. As a result, there does not appear to be an immediate need for regulatory intervention in this regard. Rather, the Commission could adopt a wait-and-see approach. Notwithstanding this, the question of how to make electronic contracts in general, and smart contracts specifically, more transparent and user-friendly is one of general importance in the Digital Single Market. As such, the Commission could also encourage related research funding for projects seeking to achieve this objective.

Then, for *smart contract arbitration mechanisms*, it was concluded that it is at present too early to determine whether requirements to file documents in national courts merely seek to achieve public policy objectives in a technology-neutral manner or whether they might unduly limit the development of smart contract arbitration mechanisms in the EU. A wait-and-see approach could thus provide further clarity in this respect. The Commission could, however, also encourage the adoption of standard arbitration clauses to assist and help businesses in this regard.

Lastly, in relation to smart contracts and *notarisation*, it is recommended that the European Commission continues to monitor developments in this field in order to determine whether existing rules are pertinent for the protection of given public policy objectives and apply in a technology-neutral manner, or whether it may be necessary to revise these rules.

Utility tokens

In terms of the policy option with respect to legal issues regarding utility tokens, the analysis shows that European regulators could consider two policy options regarding the *lack of legal certainty and regulatory fragmentation*: they could reduce uncertainty and fragmentation through the issuing of regulatory guidance as to how related legal frameworks apply to utility tokens, or consider the creation of a supranational regime on utility tokens.

Secondly, with regard to the application of *consumer protection rules* (including prospectus requirements) to utility tokens, the research showed that although consumer protection law applies to utility tokens, there often appears to be a lack of awareness that this is the case, and different forms of implementation in Member States have led to fragmentation in the internal market. In this respect, the Commission could encourage the adoption of standards by industry which may subsequently be endorsed by regulation. Moreover, the adoption of guidance by the European Commission and/or national authorities regarding how exactly consumer protection law applies to utility tokens would appear to be a useful step.

Lastly, regarding the *trading of utility tokens on secondary markets*, many stakeholders highlighted that there is a lack of legal clarity concerning the trading of utility tokens on secondary markets. To address this matter, the Commission could adopt regulatory guidance on the rules applicable where utility tokens are traded on secondary markets and encourage the adoption of standards by industry that are subsequently endorsed by regulation if need be.

The below policy matrix summarises the findings set out above.

Policy matrix

	Wait-and-See	**Regulatory Guidance**	**Secondary Legislation**	**Other (e.g. research funding, opt-in regime, regulatory sandboxes, monitoring, best practices, standard terms and conditions or model contracts)**
Legal issues regarding blockchain technology in general				
Responsibility for legal compliance and liability	X			
Potential barriers in sectoral (e.g. AML) legislation	X			X
The protection of fundamental legal principles and mandatory rules	X			X
Tension between blockchain reality and legal reality	X	X		X
Legal issues regarding smart contracts				
Application of Contract Law	X			X
The need for written form of the contract	X			
Smart contracts and Consumer Law	X	X		X
Smart contracts and pseudonymity				X
Smart contracts and jurisdiction	X			X
Capacity to contract and the protection of minors	X			X
Opacity	X			X
Smart Contract Arbitration Mechanisms				X
Notarisation	X			X
Legal issues regarding utility tokens				
The lack of legal certainty and regulatory fragmentation		X	X	
Consumer protection (including prospectus requirements)	X	X		X
Trading on secondary markets		X		X

Analysis of the impact of blockchain technology on the economy and society

Many commentators have asserted that blockchain will contribute to economic growth and foster local social development. This Study fills a major void in blockchain research by forecasting the qualitative and quantitative socio-economic benefits of blockchain. The Study draws on extensive research and more than 100 experts have contributed to the study.

The Study provides an insight to a probable scenario if Europe can maximise the benefits of blockchain. Forecasts have adopted conservative estimates and all assumptions are clearly presented to enable transparency in predictions. These forecasts were shared with experts using Delphi methods to validate and/or adjust predictions to more accurately reflect the views of blockchain professionals.

Policies should enhance blockchain drivers and address barriers restricting the many socio-economic benefits that could arise from blockchain. The insights to change, provided in forecasts to 2030 will provide policymakers with a richer understanding of potential futures.

During the research, 'legal certainty' and 'regulation clarity' were regarded as key catalysts for blockchain development. Interestingly, since this certainty and clarity does not currently exist in all areas, the same two issues were highlighted as key barriers by some observers.

The Study examined the stakeholder groups and sectors most likely to be impacted by blockchain. A number of studies assert that the largest impacts of blockchain will arise in the financial sector. The World Economic Forum highlighted that many liquid and illiquid financial assets remain highly dependent on intermediating institutions to discover and connect buyers and sellers, often based on networks of pre-existing relationships with other institutions. Blockchain capabilities have the potential to support market making and disintermediation. A number of financial platforms are emerging that realign how buyers and sellers are connected for various products and transactions, generally improving the efficiency of those markets.

Research developed baseline forecasts. These baselines were developed to investigate the impact of policy options on blockchain market expenditure and intra-EU trade facilitated by smart contracts. The baseline models are a meta-analysis best estimate of the future. Baseline models were developed during two rounds of Delphi research with more than 200 global experts. Delphi participants estimated blockchain expenditure of between €10.06 billion and €10.98 billion in 2030. Participants also estimated there would be up to 102 million blockchain supported smart contract intra-EU transactions for goods in 2030.

To investigate the impact of the proposed policy options ('Wait and See', Regulatory Guidance and Secondary Legislation) on the baseline forecasts, research adopted guidelines from the European Commission Better Regulation Toolbox. Research used relevant DG CONNECT Impact Assessments since 2017 (that had been positively received by the Regulatory Scrutiny Board) to provide robust insights into the expected impacts and costs of complementary policies. Timescales for policy implementation were found by examining policy implementation timelines for previous legislation associated with Connected Digital Single Market activities. Implementation generally took between one and two years.

12 of the 16 policy options proposed adopted a 'wait and see' approach. We believe this monitoring would be undertaken during the course of Commission's everyday activities.

No costs were associated with these activities. Costs associated with three broad policy option areas (i.e. blockchain technology in general, smart contracts and utility tokens) included:

Legal issues regarding blockchain technology in general: Regulatory guidance is suggested to address the tension between blockchain reality and legal reality. Guidance, to be led by the European Commission, but with input from Member State governments, industry groups and other stakeholders is estimated to take one or two years to implement at estimated costs of €210,900 and €421,800 respectively.

Comparison of the impact of these polices with the baseline model for blockchain expenditure across all EU28 Member States estimated cumulative annual impacts between 2020 and 2030 of €2.89 billion if the impact of the policy option is two per cent per annum and €4.38 billion if the policy has a three per cent impact.

Legal issues regarding smart contracts: Regulatory guidance is suggested to address regulatory issues concerning smart contracts. Like the previous group of policy options, the development of regulatory guidance by the European Commission with input from Member State governments, industry groups and other stakeholders is estimated to take one or two years to implement at estimated costs of €210,900 and €421,800 respectively.

The impact of policies providing guidance for smart contracts on intra-EU trade is estimated to lead to cumulative transaction savings between 2022 and 2030 of between €160 million and €242 million.

Policy options for ***utility tokens*** are the only area in which the introduction of secondary legislation is envisaged. The development and implementation of secondary legislation over a two to five year period is estimated to cost €4.7 million. Three policy guidance options were also proposed. Total policy option implementation costs in this area are estimated to be €4.922 million.

An expert workshop for this Study in Brussels in December 2019 highlighted difficulties in defining 'utility tokens' and in providing functional and legal criteria for tokens. It was also noted that tokens can take on a hybrid nature overlapping with financial tokens. With this fluidity in definitions and parameters, it was not possible to develop a relevant and robust baseline model against which to estimate policy impacts.

It is evident from the above policy implementation costs estimates and impacts on baseline models that the benefits of the policy options hugely outweigh costs. Adopting the lowest impact predictions and highest policy option implementation costs, the benefits outweigh policy costs more than 500 times.

Document de Synthèse

Ce document constitue le rapport final de l'« Etude sur les Blockchains : aspects juridiques, de gouvernance et d'interopérabilité (SMART 2018/0038) », (ci-après dénommée « l´Étude ») réalisée par Spark Legal Network, Michèle Finck, Tech4i2 et Datarella (ci-après collectivement dénommés le « Consortium »), pour la Direction Générale des Réseaux de Communication, du Contenu et de la Technologie de la Commission Européenne, Direction F : Marché Numérique Unique, Unité F3 : Innovation Numérique et Blockchain.

Objectifs et méthodologie

L'objectif global de l'Etude est de fournir des preuves et un soutien aux approches politiques et aux actions concrètes dans le cadre de l'initiative européenne « Blockchain » et de contribuer à l'élaboration d'une stratégie de l'UE, à la lumière de l'évolution de la blockchain. L'Etude analyse et évalue donc le cadre juridique de l'UE concernant la technologie blockchain et présente des options stratégiques lorsqu'un besoin d'ajustement ou de clarification est nécessaire. L'Etude évalue également quels seraient les impacts de la blockchain et de ces options stratégiques, en vue d'examiner les potentiels développements politiques futurs de la blockchain.

Collecte de données

Afin d'atteindre les objectifs susmentionnés, des données ont été recueillies par le biais de recherches documentaires et d'enquêtes sur le terrain. En ce qui concerne les recherches documentaires, toute la littérature pertinente pour l'Etude a été consultée par le Consortium afin d'identifier et d'apprécier le contexte technique, économique et de gouvernance applicable à la technologie blockchain et d´acquérir une meilleure compréhension des questions juridiques concernant cette dernière. En outre, une équipe d'experts juridiques nationaux a rempli un questionnaire de recherche juridique, couvrant la France, l'Allemagne, l'Italie, l'Espagne, le Royaume-Uni (y compris Gibraltar), les États-Unis, la Suisse et Singapour. Les questionnaires de recherche juridique complétés montrent de manière comparable comment les cadres réglementaires nationaux abordent les aspects clés pertinents à la blockchain et facilitent une meilleure compréhension des règles et réglementations juridiques pertinentes dans ces pays.

De plus, le Consortium a mené des recherches sur le terrain au moyen de deux types d'entretiens. Une première session d'entretiens a été menée auprès des principaux acteurs du domaine de la blockchain, à savoir des (représentants) d'organisations industrielles et socio-économiques, des sociétés de capital-risque et des experts juridiques et/ou des cabinets d'avocats traitant régulièrement de la blockchain. Le deuxième type d'entretiens a eu lieu avec des représentants des régulateurs nationaux financiers. Au cours de ces entretiens, l'opinion des personnes interrogées a été sollicitée sur la réglementation des « utility token[1] ICOs[2] ».

Définition du contexte technique, économique et de gouvernance applicable à la technologie blockchain

Afin d'obtenir une image globale de certains des aspects les plus importants de la technologie blockchain – notamment les opportunités et risques liés à cette technologie – le contexte technique, économique et de gouvernance applicable à la technologie

[1] Jeton d'utilité
[2] Initial Coin Offerings : offres initiales de pièces

blockchain a été examiné par le Consortium. Dans un premier temps, cela a impliqué l´examen du contexte technique, l´exposition de ce que la technologie blockchain constitue et implique exactement et la détermination de quelles en sont les variétés. Deuxièmement, les questions de capacité de transaction, les préoccupations environnementales et la notion de cybersécurité ont été prises en considération. Enfin, les questions d'intégration aux systèmes existants, d'interopérabilité et de normalisation, de jetonisation comme moyen d'incitation, et d'organisation et de gouvernance ont été étudiées.

Identification des problèmes juridiques de la technologie blockchain

Après avoir établi le contexte, un certain nombre de questions juridiques générales relatives à la technologie blockchain ont été identifiées et examinées. La première de ces questions concerne la charge de la conformité et responsabilité juridique. La seconde concerne les potentiels obstacles à la législation sectorielle pouvant empêcher la blockchain de libérer son potentiel socio-économique dans l'UE, et l'impact potentiel de la DLT (la technologie des registres distribués) sur les règles de conservation des données, telles que celles découlant de la directive sur la lutte contre le blanchiment d'argent. La troisième question examinée concerne la protection des principes juridiques fondamentaux et des règles impératives. En effet, la DLT peut également être utilisée pour enfreindre les principes juridiques fondamentaux ou des règles impératives (tels que la prohibition de la pédopornographie, du trafic de drogue et le blanchiment d'argent) et il peut être difficile de supprimer le contenu connexe de la base de données. Enfin, le quatrième aspect juridique identifié concerne la tension entre la réalité de la blockchain et la réalité juridique. Il peut y avoir des situations, par exemple, où, d'un point de vue juridique, la propriété change, mais cela ne se reflète pas sur la chaîne.

En outre, un certain nombre de questions juridiques concernant les contrats intelligents ont été identifiées par le Consortium, à commencer par l'application du droit des contrats. En l'espèce, il a été observé que le droit des contrats s'applique aux contrats intelligents à condition qu'ils soient effectivement considérés comme des contrats juridiques. Une attention particulière a été accordée à la dimension transfrontalière des contrats intelligents. Les exigences légales nationales relatives à la nécessité d'une forme écrite du contrat ont, ensuite, été prises en considération. Troisièmement, l'application du droit de la consommation aux contrats intelligents a été discutée. En effet, les transactions automatisées, caractérisées par une grande complexité, peuvent être problématiques, car les non-experts peuvent avoir des difficultés à comprendre ce que le contrat intelligent transpose au niveau technique. Toutefois, les contrats intelligents présentent également d'éventuelles opportunités du point de vue de la protection des consommateurs. Par la suite, la question des contrats intelligents et du pseudonymat a été identifiée et examinée. À cet égard, le pseudonymat présente des avantages (vis-à-vis de la protection des données par exemple) et des inconvénients (notamment au regard de la lutte contre le blanchiment d'argent) du point de vue juridique. La cinquième question évaluée est celle des contrats intelligents et de la compétence. Les blockchains sont utiles à la coordination des actions entre différents acteurs, qui peuvent être situées à divers endroits, soulevant des questions de droit applicable et de compétence juridictionnelle. Par ailleurs, la question de la capacité à contracter et la protection des mineurs a également été évaluée. Dans la situation où on ne sait pas si une partie est incapable ou si une personne mineure est impliquée, il est impossible de déterminer si cette partie a la capacité de contracter. Le septième aspect juridique examiné est celui de l'opacité. Se pose la question de savoir comment les parties qui n'ont pas les connaissances techniques nécessaires peuvent-elles négocier, rédiger et juger les contrats intelligents. Les mécanismes d'arbitrage en matière de contrats intelligents et en particulier la question de la compatibilité entre ces mécanismes et les exigences juridiques vis-à-vis des procédures d'arbitrage ont été

évalués. Enfin, le Consortium a étudié l'impact potentiel des contrats intelligents sur la notarisation. De nombreux acteurs interrogés ont fait valoir que la DLT pourrait faciliter la tâche de la profession notariale en raison de sa résistance à la falsification et la possibilité de coordination par le biais de plusieurs parties. Cependant, il a été parfois mentionné la crainte que les exigences légales relatives à la notarisation n'empêchent la conclusion des transactions numériques par des moyens purement numériques.

Les questions juridiques relatives aux jetons d'utilité ont également été mises en avant. Le manque de sécurité juridique quant à la façon dont divers cadres juridiques existants devraient être appliqués aux cas d'utilisation de la blockchain et à la fragmentation de la réglementation a été examiné en détail. Par ailleurs, l'application du droit de la protection des consommateurs ainsi que les exigences en matière de prospectus ont été étudiés vis-à-vis des jetons d'utilité. Enfin, la question des transactions sur les marchés secondaires a également été discutée. Certains acteurs ont souligné que s'il existe un marché secondaire pour les jetons, il en résulte un risque d'abus de marché (comme les opérations d'initiés et la manipulation du marché). En ce qui concerne les jetons d'utilité, il y a aussi un risque que ceux-ci soient achetés comme un investissement spéculatif (ce qui pourrait ensuite les transformer en un titre sur le marché secondaire).

Présentation des options stratégiques

Par la suite, le Consortium a identifié les différentes options stratégiques à disposition de la Commission européenne. Plus précisément, les approches suivantes ont été discutées : l'attentisme, l'adoption de lignes directrices mais également la possibilité de nouvelles règles supranationales de droit dérivé, un régime « opt-in », ainsi que des « sandboxes »[3] de régulation. Chaque option stratégique a été introduite de façon descriptive et leurs avantages et inconvénients respectifs sont ensuite étaient détaillés.

Analyse juridique et socio-économique

Dans le cadre de l'analyse juridique, les différentes options stratégiques ont été évaluées et développées afin de répondre aux questions identifiées vis-à-vis de la technologie blockchain, des contrats intelligents et des jetons d'utilité, le but étant de répondre au potentiel besoin d'ajustement ou de clarification du cadre juridique et politique et de permettre à l'UE de continuer à favoriser un secteur de la blockchain conforme et compétitif au niveau international. Afin de valider les résultats et les options stratégiques préliminaires, un séminaire a été organisé le 2 décembre 2019, regroupant les principaux acteurs du secteur. Sur la base des commentaires reçus lors de ce séminaire, le Consortium a affiné et finalisé ses conclusions.

En outre, l'impact de la technologie blockchain sur l'économie et sur la société a été évalué. Cette analyse économique examine comment les services évolueront et donne un aperçu de l'impact des options stratégiques sur l'économie et la société.

Les résultats de l'analyse juridique et socio-économique sont présentés plus en détail ci-dessous.

[3] Bac à sable

Évaluation des options stratégiques à la lumière des questions juridiques relatives à la technologie blockchain

Questions juridiques générales relatives à (au développement de) la blockchain

Tout d'abord, en ce qui concerne les questions juridiques générales qui ont été soulignées vis-à-vis de la technologie blockchain, il a été constaté qu'en termes de *charge de la conformité et responsabilité juridique,* les principaux défis ne sont pas dus aux lacunes des cadres juridiques respectifs, mais plutôt au fait que les systèmes de blockchain et leurs cas d'utilisation spécifiques n'auraient pas été conçus en vue de se conformer aux exigences légales. Par conséquent, le Consortium considère qu'aucune réponse politique spécifique n'apparaît nécessaire et recommande à la Commission d'adopter une approche attentiste. En outre, une meilleure conception technique et de gouvernance pourrait permettre une plus grande conformité. Bien que cette tâche n'incombe pas en premier lieu aux pouvoirs publics, la Commission pourrait néanmoins encourager les efforts de l'industrie à cet effet. Enfin, une application plus stricte de la loi par les agences nationales et supranationales compétentes soulignerait que le respect des règles n'est pas facultatif et inciterait l'industrie à s'y conformer.

En ce qui concerne la problématique des *obstacles potentiels dans la législation sectorielle*, il est constaté que le respect de la législation pour la lutte contre le blanchiment d'argent est essentiellement une question de gouvernance (pour l'acteur utilisant la blockchain) ainsi qu'une question d'application effective des réglementations existantes (du point de vue de l'autorité publique) et qu'ainsi, une réponse politique spécifique vis-à-vis de cette question juridique n'apparaît pas nécessaire. Il est suggéré que la Commission adopte une approche attentiste. Toutefois, dans l'hypothèse où la Commission souhaiterait adopter une approche plus active, elle pourrait encourager de manière proactive l'industrie à concevoir des systèmes de lutte contre le blanchiment d'argent basés sur la blockchain afin d'assurer le respect de la réglementation existante d'un point de vue technique, par exemple par le biais du financement de la recherche. En outre, l'adoption de conditions générales ou de contrats types pourrait être utilisée pour coordonner la conformité (tels que des contrats types assurant que les échanges d'information entre les nombreuses parties à des fins de lutte contre le blanchissement d'argent soient respectés).

En ce qui concerne la *protection des principes juridiques fondamentaux et des règles impératives*, les recherches ont révélé que les principes existants semblent bien adaptés pour résoudre les problèmes liés à l'utilisation criminelle de cette technologie. Il n'y a donc pas de besoin immédiat d'une action politique concrète et il a été considéré que la Commission européenne devrait adopter une approche attentiste.

Le Consortium a estimé que la tension entre la *réalité de la blockchain et la réalité juridique* s'assimile à une question de conception technique et de gouvernance humaine, qui n'est pas propre à la blockchain. Les recherches révèlent donc qu'il n'y a pas de besoin immédiat d'action politique et le Consortium recommande l'adoption d'une approche attentiste dans ce contexte. Dans le cas où la Commission souhaiterait d'ores et déjà adopter une approche plus proactive, elle pourrait encourager le développement de solutions techniques et de gouvernance visant à aligner l'information sur la chaîne et hors chaîne (tels que des lignes directrices en matières de pratiques exemplaires) et à fournir un financement à la recherche pour des projets visant à résoudre ces problématiques (qui sont également pertinents pour l'économie numérique de manière plus générale).

Contrats intelligents

En ce qui concerne les contrats intelligents, l'Etude a montré que si ces derniers ne sont pas toujours des contrats juridiques, ils peuvent néanmoins être considérés comme tel lorsqu'ils répondent à la définition pertinente d'un contrat valide dans la législation nationale. Aux vues du résultat des recherches, la question de *l'application du droit des contrats* aux contrats intelligents n'est pas considérée comme une source de préoccupation par les acteurs concernés. Par conséquent, aucune mesure spécifique n'est nécessaire à ce stade, et il est suggéré que la Commission adopte une approche attentiste. En ce qui concerne le cas spécifique des transactions transfrontalières, il se peut qu'un contrat valide dans le cadre d'une juridiction ne le soit pas dans une autre, et il existe une certaine incertitude quant à la question de savoir si l'article 3(1) du règlement Rome I puisse s'appliquer aux actifs basés sur la blockchain. Bien que cette question doive être clarifiée par la Cour de Justice de l'Union européenne ou par une révision du règlement Rome I à terme, il pourrait être bénéfique que la Commission édicte d'ores et déjà des lignes directrices réglementaires.

Par ailleurs, les recherches ont révélé que *les dispositions nationales du droit des contrats exigeant un contrat écrit*, qui s'appliquent dans certaines circonstances, semblent fonctionner de manière technologiquement neutre pour protéger des objectifs politiques importants. De plus, dans de nombreux cas, ces exigences peuvent être satisfaites lorsque le contrat est sous forme électronique. Il est donc recommandé à la Commission d'adopter une approche attentiste.

De plus, étant donné que les acteurs interrogés n'ont pas signalé de problèmes juridiques spécifiques liés à l'application du droit de la consommation aux contrats intelligents, la Commission pourrait adopter une approche attentiste. En ce qui concerne la question spécifique du droit de rétractation, conformément à la directive sur les droits des consommateurs, la Commission pourrait engager une discussion sur la question de savoir si les droits de rétractation des consommateurs créent une charge excessive sur les contrats intelligents, dans le cadre de la prochaine révision de ce régime juridique (conformément au considérant 62 de la directive sur les droits des consommateurs). Entre-temps, la Commission pourrait également choisir d'adopter des lignes directrices réglementaires sur la manière précise dont le droit de la protection des consommateurs s'applique aux contrats intelligents.

En ce qui concerne les *contrats intelligents et le pseudonymat,* la Commission pourrait encourager l'adoption de clauses contractuelles types relatives à l'identification des parties contractantes. Au-delà de cette possibilité, la Commission pourrait également surveiller cette problématique et, si elle le juge approprié, encourager le développement de systèmes numériques et/ou de SSI, en finançant la recherche par exemple.

Vis-à-vis des *contrats intelligents et la juridiction compétente*, les législations supranationales existantes telles que les régimes sous Bruxelles I et de Rome I semblent bien adaptées pour régir les questions connexes, de sorte que l'adoption d'une approche attentiste semble bien adaptée dans ce domaine.

Au regard de la *capacité de contracter et les mineurs*, il ne semble pas y avoir de besoin immédiat d'intervention réglementaire dans le domaine, favorisant le choix d'une approche attentiste. La Commission pourrait toutefois subventionner la recherche pour des projets visant à fournir des solutions novatrices.

Concernant la question de *l'opacité*, le droit dérivé supranational existant semble déjà contenir des mécanismes permettant de remédier aux inconvénients que l'opacité peut générer pour les consommateurs. Par conséquent, il ne semble pas y avoir un besoin

immédiat d'intervention réglementaire à cet égard. La Commission pourrait ainsi adopter une approche attentiste. Cependant, la question de savoir comment rendre les contrats électroniques en général, et les contrats intelligents en particulier, plus faciles à comprendre est d'une importance générale dans le marché numérique unique. À ce titre, la Commission pourrait également encourager le financement de recherches pour des projets visant à atteindre cet objectif.

Ensuite, en ce qui concerne *les mécanismes d'arbitrage des contrats intelligents,* il a été conclu qu'il est actuellement trop tôt pour déterminer si l'obligation de déposer des documents devant les tribunaux nationaux vise simplement à atteindre des objectifs d'ordre public d'une manière technologiquement neutre ou si elle risque de limiter indûment le développement des mécanismes d'arbitrage des contrats intelligents dans l'UE. Une approche attentiste pourrait donc apporter davantage de clarté dans ce contexte. La Commission pourrait toutefois également encourager l'adoption de clauses d'arbitrage types pour aider et assister les entreprises à cet égard.

Enfin, vis-à-vis des contrats intelligents et la *notarisation*, il est recommandé que la Commission européenne continue de suivre l'évolution de la situation dans ce domaine afin de déterminer si les règles existantes sont pertinentes pour la protection des objectifs de politique publique donnés et s'appliquent de manière neutre sur le plan technologique, ou s'il apparaît nécessaire de réviser ces règles.

Jetons d'utilité

En ce qui concerne l'option stratégique relative aux questions juridiques concernant les jetons d'utilité, l'analyse montre que les régulateurs européens pourraient envisager deux options stratégiques vis-à-vis du *manque de sécurité juridique et la fragmentation réglementaire* : ils pourraient réduire l'incertitude et la fragmentation en publiant des lignes directrices réglementaires sur la manière dont les cadres juridiques connexes s'appliquent aux jetons d'utilité, ou envisager la création d'un régime supranational sur les jetons d'utilité.

Par ailleurs, concernant l'application des règles de *protection des consommateurs* (y compris les exigences en matière de prospectus) aux jetons d'utilité, les recherches ont démontré que, bien que la législation relative à la protection des consommateurs s'applique aux jetons d'utilité, il semble souvent que les parties prenantes n'en soient pas conscientes, et que les différentes formes de mise en œuvre dans les États membres ont entraîné une fragmentation du marché intérieur. À cet égard, la Commission pourrait encourager l'adoption de normes par l'industrie, qui pourraient ensuite être entérinées par une règlementation. En outre, l'adoption de lignes directrices par la Commission européenne et/ou les autorités nationales concernant la manière précise dont la législation sur la protection des consommateurs s'applique aux jetons d'utilité semblerait être une étape utile.

Enfin, au regard des échanges de jetons d'utilité sur les marchés secondaires, de nombreux acteurs ont souligné le manque de clarté juridique en la matière. Pour remédier à ce problème, la Commission pourrait adopter des lignes directrices réglementaires sur les règles applicables aux échanges de jetons d'utilité sur les marchés secondaires et encourager l'adoption de normes par l'industrie, qui seraient ensuite approuvées par voie réglementaire si nécessaire.

La matrice politique ci-dessous résume les conclusions exposées ci-dessus.

Matrice des politiques

	Attentisme	Lignes directrices réglementaires	Droit dérivé	Autres (p. ex. financement de la recherche, régime d'opt-in, sandboxes réglementaires, surveillance, pratiques exemplaires, conditions générales standardisées ou contrats types)
Questions juridiques concernant la technologie blockchain en général				
Charge de la conformité et responsabilité juridique	X			
Obstacles potentiels dans la législation sectorielle (p. ex. la lutte contre le blanchiment d'argent)	X			X
La protection des principes juridiques fondamentaux et des règles impératives	X			X
Tension entre la réalité de la blockchain et la réalité juridique	X	X		X
Questions juridiques concernant les contrats intelligents				
Application du droit des contrats	X			X
La nécessité d'une forme écrite du contrat	X			
Contrats intelligents et droit de la consommation	X	X		X
Contrats intelligents et pseudonymat				X
Contrats intelligents et juridiction compétente	X			X
Capacité de contracter et protection des mineurs	X			X
Opacité	X			X
Mécanismes d'arbitrage en matière de contrats intelligents				X
Notarisation	X			X
Questions juridiques concernant les jetons d'utilité				
Le manque de sécurité juridique et la fragmentation réglementaire		X	X	
Protection du consommateur (y compris les exigences en matière de prospectus)	X	X		X
Transactions sur les marchés secondaires		X		X

Analyse de l'impact de la technologie blockchain sur l'économie et la société

De nombreux acteurs ont affirmé que la blockchain contribuerait à la croissance économique et favoriserait le développement social local. Cette Etude comble un important vide en matière de recherche sur la blockchain en envisageant les avantages socio-économiques qualitatifs et quantitatifs de la blockchain. L'Etude s'appuie sur des recherches approfondies et la contribution de plus de 100 experts.

L'Etude fournit un aperçu d'un scénario pouvant survenir si l'Europe parvient à maximiser les avantages de la blockchain. Les prévisions ont été identifiées selon des estimations prudentes et toutes les hypothèses sont clairement présentées pour permettre la transparence de ces prédictions. Ces dernières ont été partagées avec des experts utilisant des méthodes Delphi pour valider et / ou ajuster les prévisions afin de refléter plus précisément les points de vue des professionnels de la blockchain.

Il a été établi que les politiques devraient améliorer les moteurs de la blockchain et éliminer les obstacles limitant les nombreux avantages socio-économiques qui pourraient découler de la blockchain. Les informations sur cette évolution, fournies dans les prévisions, allant jusqu'en 2030, permettront aux décideurs politiques de mieux comprendre le potentiel avenir de cette technologie.

Au cours des recherches, la « sécurité juridique » et la « clarté de la réglementation » ont été considérées comme les principaux catalyseurs du développement de la blockchain. Il est intéressant de noter que la sécurité et la clarté n'existent pas actuellement dans tous les domaines. Toutefois, ces deux mêmes notions ont été identifiées comme obstacles clés par certains observateurs.

L'Etude a examiné les groupes d'acteurs et les secteurs les plus susceptibles d'être touchés par la blockchain. Un certain nombre d'études affirment que les impacts les plus importants de la blockchain se produiront dans le secteur financier. Le Forum Économique Mondial a souligné que de nombreux actifs financiers liquides et non liquides restent fortement dépendants des institutions intermédiaires pour découvrir et connecter les acheteurs et les vendeurs, souvent sur la base de réseaux de relations préexistantes avec d'autres institutions. Les capacités de la blockchain ont le potentiel de soutenir la création de marché et la désintermédiation. Un certain nombre de plates-formes financières émergeantes réalignent la façon dont les acheteurs et les vendeurs sont connectés pour divers produits et transactions, améliorant généralement l'efficacité de ces marchés.

Les recherches ont permis de développer des prévisions de référence. Ces bases de référence ont été élaborées pour étudier l'impact des options stratégiques sur les dépenses du marché de la blockchain et la facilitation du commerce intra-UE par les contrats intelligents. Les modèles de référence constituent une méta-analyse des meilleures estimations de l'avenir. Des modèles de référence ont été développés au cours de deux cycles de recherche Delphi, comptant la participation de plus de 200 experts mondiaux. Les participants aux recherches Delphi ont estimé les dépenses liées à la blockchain entre 10,06 milliards d'euros et 10,98 milliards d'euros en 2030. Les participants ont également estimé que les transactions de marchandises, soutenues par des contrats intelligents, représenteraient jusqu'à 102 millions d'euros en 2030.

Pour étudier l'impact des options stratégiques proposées (attentisme, lignes directrices réglementaires et droit dérivé) sur les prévisions de référence, les recherches ont été menées, suivant les lignes directrices de la Boîte à outils pour une meilleure réglementation de la Commission européenne. Des analyses d'impact pertinentes menées par la DG CONNECT depuis 2017 (qui avaient été reçues positivement par le

comité d'examen de la réglementation) ont été utilisées afin de fournir des informations solides sur les impacts et les coûts attendus des politiques complémentaires. Les délais de mise en œuvre des politiques ont été déterminés en examinant les délais de mise en œuvre des politiques vis-à-vis de législations antérieures en matière d'activités du marché numérique unique connecté. Il a été observé que la mise en œuvre prend généralement entre un et deux ans.

12 des 16 options stratégiques proposées présentent une approche « attentiste ». Il est considéré que les opérations de contrôle associées à cette approche seront effectuées au cours des activités quotidiennes de la Commission et ne représentent pas de coût particulier. Par ailleurs, les options stratégiques proposées engendrant des coûts comprennent les options suivantes (c.-à-d. technologie de la blockchain en général, contrats intelligents et jetons d'utilité) :

Questions juridiques concernant la technologie de la blockchain en général: la publication de lignes directrices réglementaires a été suggérée pour résoudre la tension entre la réalité de la blockchain et la réalité juridique. Les lignes directrices, qui seront dirigées par la Commission européenne, avec la contribution des gouvernements des États membres, des groupes industriels et d'autres parties prenantes, devraient prendre un ou deux ans à mettre en œuvre, pour des coûts estimés respectivement à 210 900 ou 421 800 d'euros.

Aux vues de la comparaison de l'impact de ces politiques avec le modèle de référence vis-à-vis des dépenses liées à la blockchain dans tous les États membres de l'UE28, il a été estimé que les impacts annuels cumulés entre 2020 et 2030 s'élèveraient à 2,89 milliards d'euros si l'impact de l'option stratégique est de 2% par an et à 4,38 milliards d'euros si la stratégique politique a un impact de 3%.

Questions juridiques concernant les contrats intelligents : des lignes directrices réglementaires ont été suggérées pour résoudre les problèmes réglementaires concernant les contrats intelligents. Comme pour le précédent ensemble d'options stratégiques, l'élaboration des lignes directrices réglementaires par la Commission européenne avec la contribution des gouvernements des États membres, des groupes industriels et d'autres parties prenantes devrait prendre un ou deux ans à mettre en œuvre, pour un coût estimé à 210 900 € ou 421 800 € respectivement.

L'impact des politiques mettant en place des lignes directrices pour les contrats intelligents sur le commerce intra-UE devrait conduire à des économies de transactions cumulées entre 2022 et 2030 comprises entre 160 et 242 millions d'euros.

Les options stratégiques pour les **jetons d'utilité** sont le seul domaine dans lequel l'introduction d'une législation de droit dérivé est envisagée. L'élaboration et la mise en œuvre du droit dérivé sur une période de deux à cinq ans devraient coûter 4,7 millions d'euros. Trois options de lignes directrices politiques ont également été proposées. Le coût total de mise en œuvre des options stratégiques dans ce domaine est estimé à 4,922 millions d'euros.

Un séminaire regroupant les experts en matière de blockchain, tenu pour cette étude à Bruxelles en décembre 2019, a mis en évidence les difficultés relatives à la définition des « jetons d'utilité » et l'identification de critères fonctionnels et juridiques pour les jetons. Il a également été noté que les jetons peuvent revêtir une nature hybride, se chevauchant avec la notion de jetons financiers. En raison de cette fluidité des définitions et paramètres, il n'a pas été possible de développer un modèle de référence pertinent et solide permettant d'estimer les impacts des politiques stratégiques.

Il ressort clairement des estimations des coûts de mise en œuvre des politiques et des impacts sur les modèles de référence que les avantages des options stratégiques l'emportent largement sur les coûts. En adoptant les prévisions d'impact les plus faibles et les coûts de mise en œuvre des options stratégiques les plus élevés, les avantages l'emportent sur les coûts politiques plus de 500 fois.

1. Introduction

This document constitutes the Final Report for the 'Study on Blockchains: legal, governance and interoperability aspects (SMART 2018/0038)' (also referred to as: the 'Study') carried out by Spark Legal Network, Michèle Finck, Tech4i2 and Datarella (together also referred to as: the 'Consortium') for the Commission's Directorate-General for Communications Networks, Content and Technology, Directorate F: Digital Single Market, Unit F3: Digital Innovation and Blockchain.

1.1. Objectives of the Study

The overall objective of the Study is to provide evidence and support for policy approaches and concrete actions within the European blockchain initiative and to contribute to the building of an EU strategy in light of blockchain developments. The Study therefore analyses and assesses the legal framework in the EU with regard to blockchain technology and presents policy options where a need for adjustment or clarification is required. The Study also assesses what the impacts of blockchain and these policy options could be with a view to consider future blockchain policy developments.

More specifically, the Consortium carried out four main tasks:

1. A literature review and desk and field research in order to assess the developments, trends and emerging issues concerning regulatory frameworks;
2. Legal analysis, with a view to identifying a number of policy options;
3. Analysis of the impact of blockchain technology on the economy and on society.
4. Experience sharing and validation of policy and recommendations via the organisation of a stakeholder workshop.

A description of the methodology that the Consortium applied during the Study follows below.

1.2. Overview of the methodology

In order to meet the above-mentioned objectives and carry out the relevant tasks, the steps set out below were undertaken.

1.2.1. Desk research

The Consortium executed two different types of desk research. Firstly, all literature relevant to the Study (a complete list of sources can be found in Annex I) was consulted in order to identify and appreciate the technical, economic and governance context applicable to blockchain technology and to gain insight into the legal issues regarding blockchain technology. In carrying out this task, the Consortium recognised that, as blockchain is a relatively young and developing technology, the regulatory framework and the legal commentary are still in a state of flux as well. Therefore, a flexible approach was taken, and new literature and ongoing regulatory developments were continually added throughout the Study.

The second type of desk research consisted of structured legal research at national level. As part of this step, a targeted legal research questionnaire with a number of key questions designed to enable a better understanding of the relevant legal rules in the selected countries (EU Member States and third countries) was created. This questionnaire covered the key topics analysed in this Study: general legal issues related to blockchain technology, smart contracts and utility tokens. National legal experts in France, Germany, Italy, Spain, the UK (including Gibraltar), the United States, Switzerland and Singapore completed the legal research questionnaire under the

guidance and instructions of the Consortium.[4] The completed legal research questionnaires show in a comparable fashion how the national regulatory frameworks address key aspects relevant to blockchain, and thereby facilitate a better understanding of the relevant legal rules in these countries. The completed legal research questionnaires can be found in Annex III.

1.2.2. Field research

Secondly, the Consortium conducted field research via two types of interviews. The first set of interviews were conducted with key stakeholders in the field. The group of stakeholders consisted of (representatives of) industry and socio-economic organisations, venture capitalists and legal experts and / or law firms dealing with blockchain on a regular basis.[5] These stakeholders provided input from a practical (i.e. which are the legal matters relevant on the ground) as well as a socio-economic perspective (i.e. what are the main economic, social and environmental benefits and barriers).

The interviews were semi-structured, with the stakeholder being free to discuss the topics they considered to be important during the first stage of the interview, and indicating which legal issues they found to be of particular relevance during the second stage of the interview. Thus, the interviews gathered the thoughts and insights of the parties being interviewed in relation to certain key topics relating to blockchain as well recorded their direct observations and experiences concerning the relevance of certain legal issues affecting or being affected by blockchain technology. The members of the Consortium arranged and carried out the interviews, and captured the interviewees' responses in interview reports. The interview reports for these interviews can be found in Annex II.

The second type of interview was held with representatives of the national financial regulators.[6] The national legal experts arranged and carried out these interviews, and drafted the interview reports. During these interviews, the national legal experts asked certain pre-determined targeted questions related to the regulation of utility token ICOs. The interview reports from these interviews provided the Consortium with clear and comparable responses from the interviewees, enabling an understanding of the precise issue of the regulation of utility token ICOs. The interview reports for these interviews can be found in Annex IX.

1.2.3. Legal analysis and organisation of a workshop

Based on these data collection exercises, the Consortium performed a detailed legal analysis. As such, it identified points of friction between current legal frameworks and DLTs and the existing barriers that need to be addressed, and evaluated whether the technology can be made compliant-by-design or whether the tension cannot be reconciled under the current status quo. In the latter scenario, non-legislative and legislative policy options that may enable the achievement of the underlying policy

[4] The EU Member States were covered by internal experts from Spark Legal Network, and the third countries by prominent legal experts in the field from Switzerland, Singapore and the US (Jörn Erbguth, Dharma Sadasivan and Andrew Bull respectively).

[5] The key stakeholders that were interviewed were the following: Nordic Blockchain Association, Crypto Valley Association, Chaineum, ConsenSys Enterprise Solutions, DWF, Hogan Lovells, Blockchain Alliance / Steptoe & Johnson LLP, Fundament Group / Bundesblock, Norwegian Consumer Council, Danish Consumer Council, Gide Loyrette Nouel, Middlesex University / ANEC, Outlier Ventures, The Marschall Plan Holding, and Impact17.

[6] The regulators that were interviewed were the following: France: Autorité des Marchés Financiers (AMF) (no interview report for this interview was annexed to this report), Germany: Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Italy: Commissione Nazionale per le Società e la Borsa (CONSOB), Spain: Comisión Nacional del Mercado de Valores (CNMV), United Kingdom: Financial Conduct Authority (FCA), Switzerland: Swiss Financial Market Supervisory Authority (FINMA) and United States: United States Securities and Exchange Commission (SEC). Please note no interview was carried out with the Monetary Authority of Singapore.

objective were identified. Thus, the legal frameworks and issues with regard to blockchain technology were analysed and assessed, and policy options were presented where a need for adjustment or clarification is required. These policy options should enable the EU to continue to nurture a compliant and internationally competitive blockchain sector. The analysis covers three distinct topics: general legal issues which arise due to the nature of blockchain technology, smart contracts and utility tokens.

In order to validate these policy options, a workshop was organised on 2 December 2019. The workshop was attended by a broad range of around 70 stakeholders, including law firms, industry representatives, universities and other research institutes, consumer organisations, public authorities, and other interested individuals. The Consortium used the workshop as an opportunity to present the preliminary findings and policy options of the Study to a broad range of stakeholders in the field and gather their thoughts and feedback. Ahead of the workshop, a workshop discussion document setting out the assessment of policy options in light of the legal issues identified was shared with all participants, ensuring they were properly prepared to provide feedback on the findings of the Consortium at that stage. The workshop itself included three breakout sessions (on blockchain technology in general, smart contracts and utility tokens) which were moderated by the Consortium. During these breakout sessions, the policy options were discussed in great detail. Based on the feedback received through the workshop, the Consortium refined and finalised its findings, thereby ensuring that the findings in this Final Report reflect the concerns of relevant stakeholders.

1.2.4. Economic analysis

The impact of blockchain technology on the economy and on society was also assessed. This analysis considers how services will evolve and examines accompanying measures to soften the blockchain transition. The task also provides an overview of the impact of policy options. The examination of environmental and socio-economic costs provides an initial impact assessment type overview and an estimate of consolidated economic benefits, of greater competitiveness on industry and of social costs. Ex-ante impact assessments are always speculative, particularly in areas where new business models will emerge; forecasts are be 'handled with care'.

1.3. Structure of the Final Report

Chapter 1 of this report discusses the technical, economic and governance context applicable to blockchain technology, allowing for an appreciation of the context in which this technology is operating – including where its opportunities and risks lie. Chapter 2 builds on this description and focusses on the legal issues which arise in the context of blockchain technology – covering both general legal issues as well as the specific legal issues relating to smart contracts and utility tokens. Chapter 3 contributes to the Study by clearly setting out the various policy options the Commission has at its disposal, thereby setting the scene for the subsequent chapter. In Chapter 4, the suitability of the policy options identified in Chapter 3 is assessed for each of the legal issues regarding blockchain technology identified in Chapter 2 – both the legal issues that apply generally with regard to the technology, as well as those relating to smart contracts and utility tokens. Chapter 5 then analyses the impact of blockchain technology in general and smart contracts and utility tokens in particular on the economy and on society. Additionally, this chapter discusses the effects of the policy options selected in Chapter 4. Lastly, the conclusion of this report provides an overview of the information and findings discussed in the report.

2. Chapter 1 – Technical, economic and governance context applicable to blockchain technology

2.1. Introduction

This chapter introduces the technical, economic and governance context applicable to blockchain technology. Firstly, it discusses the technical context by setting out what blockchain technology constitutes and entails exactly, and what varieties of blockchain there are. Then, it proceeds to cover the topics of transaction capacities, environmental concerns, and cybersecurity. With regard to the applicable economic and governance context, the chapter explores the issues of integration with legacy systems, interoperability and standardisation, tokenisation as a means to provide incentives, and organisation and governance aspects.

In doing so, this chapter provides an all-round picture of some of the most important aspects of blockchain technology – including where its opportunities and risks lie. Setting this context therefore lays the groundwork for the research undertaken in the subsequent chapters.

2.2. Technical context

2.2.1. Blockchain technology

Blockchains are a much-discussed technological innovation that, according to some, promises to inaugurate a new era of data storage and code-execution, which could in turn stimulate new business models and markets. A blockchain (or Distributed Ledger Technology – 'DLT'[7]) is essentially a distributed database that is stored on various nodes (the computers that store a copy of the database) and maintained by a consensus algorithm. Blockchains have two central characteristics. *First*, they are a database that is stored by various computers (the 'nodes').[8] The ledger's data is resilient as it is simultaneously stored on many nodes so that even if one or several nodes fail, the data goes unaffected. *Second*, blockchains also function as a platform for the execution of software.[9] As a platform for code-execution, the decentralised structure ensures that the failure of one or multiple nodes does not affect the overall execution of the software. Replication achieves that there is no central point of failure.[10]

It is important to stress from the outset that there is not one 'blockchain technology'.[11] Rather, blockchains are better seen as a class of technologies operating on a spectrum that present different technical and governance structures.[12] Rather than being a completely novel technology, DLT is better understood as an inventive combination of existing mechanisms. Indeed, nearly all of its technical components originated in academic research from the 1980s and 1990s.[13] The variety of blockchains is an

[7] Various definitions of blockchains and Distributed Ledger Technology exist, and some of these stress different technical features of these respective forms of data management. Given the nature of this Study and the lack of definitional consensus, both terminologies will be used as synonyms.
[8] For a technical overview of blockchains, see Arvind Narayanan et al, 'Bitcoin and Cryptocurrency Technologies' (2016), Princeton University Press.
[9] Smart contract platforms currently include Ethereum and Neo (public platforms) and Corda and Oracle (private platforms).
[10] This does not necessarily entail that there are no central points of attack or failure at the level of software governance.
[11] The technology was first described – although not yet labelled as 'blockchain' in Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2009) available at https://bitcoin.org/bitcoin.pdf (last access on 23 October 2019). Nakamoto is the pseudonymous inventor(s) of Bitcoin.
[12] Roman Beck, Christoph Müller-Bloch and John King, 'Governance in the Blockchain Economy: A Framework and Research Agenda' (2018), p.3.
[13] Arvind Narayanan and Jeremy Clark, 'Bitcoin's academic pedigree' (2017), Communications of the ACM, Vol. 60, No. 12, pages 36-45.

important factor that calls for careful contextual analysis to determine their respective compliance with existing legal frameworks. In our Study, we will engage with such nuance and discuss how various forms of DLT interact with the legal frameworks discussed further below.

In general, DLT can be understood as shared and synchronised digital databases that are maintained by a consensus algorithm and stored on multiple nodes. These are peer-to-peer networks with the nodes serving as the different peers.[14] As its etymology reveals, a blockchain is often structured as a chain of blocks.[15] A single block groups together multiple transactions and is then added to the existing chain of blocks through a hashing process. A hash function (or 'hash') is a one-way cryptographic function that provides a unique fingerprint that represents information as a string of characters and numbers.[16] The various blocks contain different kinds of data, which includes a hash of all transactions contained in the block (its 'fingerprint'), a timestamp, and a hash of the previous block that creates the sequential chain of blocks.[17] Because blocks are continuously added but never removed, a blockchain can be qualified as an append-only data structure. Cryptographic hash-chaining makes the log tamper-evident, which increases transparency and accountability.[18] Indeed, because of the hash linking one block to another, changes in one block change the hash of that block, as well as of all subsequent blocks. The data in the various blocks are synchronised through a consensus protocol, which determines how new blocks are added to the existing ledger. It enables the distributed network to agree on the current state of the ledger in the absence of a centralised point of control.

As already noted above, it is important to understand that DLT is both a technology for data storage and can also be a novel variant of programmable platform[19] that enables new applications such as smart contracts.[20] A blockchain ecosystem is indeed multi-layered. Blockchains themselves usually rely on the Internet to operate.[21] DLT itself provides an infrastructure for data management that either directly stores data or links to data. It can be imagined as an accounting system shared between many actors that can be used by different entities to standardise and link data and 'enable credible accounting of digital events'.[22] This serves to coordinate information between many stakeholders (such as evidence about transactions) in a decentralised fashion. It is imperative to note that while blockchains only ever store data, this data can be taken to represent anything we believe and agree it represents. Bitcoin is essentially data that is valuable because people have come to believe it is.[23] Similarly, over time other forms of digital assets have emerged that are but raw data taken to represent a good, service or entitlement. Blockchain-based assets can purely have on-chain value (as in Bitcoin) or be the avatar of a real-world asset, whether a good (such as a token representing a

[14] A 'peer' of course does not have to be a private individual but can also be a corporation. Some blockchains count both full and lightweight nodes whereby only full nodes store an integral copy of the ledger. Other nodes may only store those parts of the ledger of relevance to them.
[15] It is worth noting that as the technology evolves this structure might eventually cede way to other forms of data-storage.
[16] A broader overview of hash functions can be found below.
[17] Andreas Antonopoulos, Mastering Bitcoin (O'Reilly, 2017), xxiii.
[18] Ed Felten, 'Blockchain: What is it good for?' (26 February 2018) available at https://freedom-to-tinker.com/2018/02/26/bloc (last access on 23 October 2019).
[19] A DLT may be a programable platform. It is also possible that it may not be, and the level of programmability may vary from rudimentary to Turing complete.
[20] A smart contract essentially is self-executing software code. Smart contracts are examined in further depth just below.
[21] It would also be possible to construct a blockchain that used an alternative data transmission architecture.
[22] Roman Matzutt et al, 'A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin' (26 February 2018) available at https://fc18.ifca.ai/preproceedings/6.pdf (last accessed on 23 October 2019).
[23] Bitcoin is a cryptocurrency. It is in this context that blockchain technology was first used before inspiring many other use cases.

bike), a service (such as a voucher for a haircut) or an entitlement (such as a legal right). Seen from this perspective, distributed ledgers have the potential to disrupt the online circulation of value.[24] In addition, blockchains are a platform for the decentralised execution of software. Examples include so-called smart contracts or 'decentralised applications' (applications that reflect the decentralised structure of the underlying network).[25] These applications can take a wide variety of forms and serve a wide variety of use cases.[26] Smart contracts are one form of such software that can be executed on DLT. They have been defined as 'automated software agents hosted on blockchains that are capable of autonomously executing transactions on the triggering of certain conditions'.[27] In essence, a smart contract is self-executing and deterministic[28] computer code that automatically processes its inputs when triggered. The terminology expresses that although smart contracts are not necessarily smart (at present, they only carry out what they are programmed to do) nor contracts, they can be used in contractual settings.[29] Indeed, from a technical perspective, in trustless public blockchain networks,[30] smart contracts are simply 'computer programs that can be consistently executed by a network of mutually distrusting nodes, without the arbitration of a trusted authority'.[31] Nonetheless, smart contracts can have legal implications, such as where they are used in contractual settings, for instance to 'express the contents of a contractual agreement and operate the implementation of that content'.[32]

Automated execution is smart contracts' main value proposition. Smart contract code executes automatically and cannot be halted unless this option is specifically built into the code.[33] Even if one or a number or nodes fail, the software still executes on all remaining nodes, highlighting how blockchain achieves resilience through replication. Such automated execution enables transactions in situations devoid of human or institutional trust,[34] lowers transaction costs and reduces counterparty risk and interpretative uncertainty.[35] Once an agreement has been translated into code, the

[24] Amy Cortese, 'Blockchain Technology Ushers in "The Internet of Value', *(Cisco,* 10 February 2016), available at https://newsroom.cisco.com/feature-content?articleId=1741667 (last accessed on 23 October 2019).
[25] This terminology reflects, on the one hand, that these are applications running on an infrastructure and that they can be managed in a decentralised fashion just as the infrastructure itself.
[26] In addition, there can also be intermediary layers such as a decentralised application framework that implement their own protocols for the creation and maintenance of decentralised applications
[27] Jake Goldenfein and Andrea Leiter, 'Legal Engineering on the Blockchain: "Smart Contracts" as Legal Conduct' (May 2018), Law and Critique (Forthcoming), p.2, available at SSRN: https://ssrn.com/abstract=3176363 (last accessed on 17 December 2019).
[28] This should be true in well-written code. That said, in poorly written applications it is possible to make a real mess by using "non-deterministic functions" in a smart contract.
Example: Arshad Sarfarz, 'Why Smart Contracts in Blockchain need to avoid non-deterministic functions' (Nov 2017), available at https://dzone.com/articles/why-smart-contracts-in-blockchain-needs-to-avoid-n (last accessed on 17 December 2019).
[29] The concept was first mentioned in Nick Szabo, 'Smart Contracts: Building Blocks for Digital Markets' (1996) available at http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (last accessed on 23 October 2019).
[30] Most institutional settings use consortium chains or one type or another.
[31] Massimo Bartoletti and Livio Pompianu, 'An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns' in Michael Brenner et al (eds), *Financial Cryptography and Data Security* (Springer 2017), p.494.
[32] Florian Idelberger et al, 'Evaluation of Logic-Based Smart Contracts for Blockchain Systems' in Jose Julia Alferes et al (eds), *Rule Technologies. Research, Tools, and Applications* (Springer 2016), p.167.
[33] We return to such options below.
[34] It should be noted that having no humans in the loop can give rise to problems as well. The intended behaviour and actual behaviour of a decentralised autonomous organisation can differ greatly.
[35] For an overview of smart contracts' advantages, see Mark Giancaspro, 'Is a "smart contract" really a smart idea? Insights from a legal perspective' (2017) 33 Computer Law & Security Review 825; Richard Holden and Anup Malani, 'Can Blockchain Solve the Holdup Problem in Contracts?' (2017), available at https://www.law.northwestern.edu/research-faculty/colloquium/law-economics/documents/Malani_Blockchain.pdf (last accessed on 23 October 2019), p.21-24.

intervention of a party or intermediary (other than the oracle[36]) triggering contractual execution is replaced by the software's automated execution. The software can be used for the automatic transfer of collateral in the event of default or to disburse employee compensation if performance goals are achieved.[37] Other uses for smart contracts lie in InsurTech for event-driven insurance.[38]

2.2.2. Varieties of blockchain

There is a very large variety of blockchains. Immense variety characterises their technical and functional configuration as well as their internal governance structures.[39] Different forms of DLT have different rules regarding the visibility and identifiability of transactions on the ledger and the right to add new data. Conventionally, DLT is often grouped in two categories of 'public and permissionless' and 'private and permissioned'.[40] In public and permissionless blockchains, anyone can entertain a node by downloading and running the relevant software. There are no identity restrictions for participation.[41] Transparency is moreover an important feature as anyone can download the entire database and view transaction data (which is why they are referred to as 'public' blockchains). For example, any interested party can create a Bitcoin or Ethereum (both are permissionless systems) account using public-private key cryptography without the need for prior permission from a gatekeeper. Permissionless blockchains rely on open source software that anyone can download to participate in the network. The public auditability of these ledgers enhances transparency but minimises privacy.

Private and permissioned blockchains run on a private network such as intranet or a VPN and an administrator needs to grant permission to actors wanting to maintain a node. The key distinction between permissioned and unpermissioned blockchains is indeed that while one needs access permission to join the former, this is not necessary in respect of the latter. Whereas unpermissioned blockchains are often a general-purpose infrastructure, permissioned ledgers are frequently designed for a specific purpose. These systems are not open for anyone to join and see. Rather a single party or a consortium acts as a gatekeeper. Permissioned blockchains can be internal to a specific company or joint venture (which is why they are also often referred to as 'private', 'consortium' or 'enterprise' blockchains). While public and permissionless blockchains are pseudonymous networks, in permissioned systems parties' identity is often known.[42] DLT's different characteristics impact on their relationship with the law. It is for this reason that we will distinguish between different forms of DLT in our analysis.

Furthermore, blockchains' tamper-evident nature must be stressed. It is often stated that distributed ledgers are 'immutable'. This is misleading as the data contained in such networks can indeed be manipulated in extraordinary circumstances.[43] Indeed, various participants can collude to change the current state of the ledger, meaning that while such efforts would be extremely burdensome and expensive, they are not impossible.[44]

[36] An oracle can be one or multiple persons, groups or programs that feed the software relevant information, such as whether a natural disaster has occurred (to release an insurance premium) or whether online goods have been delivered (to release payment).
[37] David Yermack, 'Corporate Governance and Blockchains' (2017) 21 Review of Finance 7, p.26.
[38] Stan Higgins, 'AXA Is Using Ethereum's Blockchain for a New Flight Insurance Product' (*coindesk,* 13 September 2017) available at https://www.coindesk.com/axa-using-ethereums-blockchain-new-flight-insurance-product (last accessed on 23 October 2019).
[39] Blockchain governance refers to the process of maintaining the software.
[40] It is worth noting that there can also be hybrids of these two most common categories.
[41] This is true at least in theory as over time informal restrictions for participation in mining (of an economic nature) and software governance have emerged.
[42] Often, but not always. In some cases, private transactions may be explicitly required.
[43] See also Conte de Leon, 'Blockchain: Properties and Misconceptions', p.290.
[44] Angela Walch, 'The Path of the Blockchain Lexicon (and the Law)', 36 Review of Banking and Financial Law, 2017, p.713.

Nonetheless, DLT is tamper-evident nature means there are often 'no technical means, short of undermining the integrity of the entire system, to unwind a transfer'.[45] Because blocks are linked through hashes, changing information on a blockchain is difficult and expensive. This creates regulatory challenges as information on DLT can in principle not be changed (such as to comply with a court order) and smart contracts' execution can in principle not be halted even where required by law (at least in a public permissionless chain). In a private permissioned chain such modifications are much easier. In a consortium chain it would be more difficult.

2.2.3. Transaction capacities

One of the main technical challenges with regard to blockchain is the question of how many transactions per second a blockchain can process (i.e. the scalability problem). This issue is the most problematic in public, permissionless blockchains, and can be said to constitute a trilemma according to which blockchains can generally have only two of the following three properties: scalability, decentralisation or security. If a blockchain is to be highly decentralised and highly secure, as a result there will be issues with its scalability. If it is highly performant and highly decentralised, it will not be secure. By the same token, blockchains that are centralised, can be highly secure and performant.[46]

The question of transaction capacities affects the extent to which blockchain technology can be used in order to carry out, for example, payments and advertising, but also whether a blockchain can be viable for large-scale applications and projects in finance, insurance, health care, etc. Furthermore, transaction speed is also very relevant when blockchain is applied in the supply chain in order to handle IoT data, for example, which requires extremely low transaction times.

Thus, transaction speed plays a big part in determining whether mass adoption of blockchain will take place or not. This can be illustrated by the example of blockchain-driven payments – either with traditional means or cryptocurrencies. In 2018, 500 billion non-cash transactions were executed around the world.[47] However, whereas VISA has a transaction capacity of 65,000 per second[48] to process such transactions, Bitcoin can only carry out 4.7 transactions per second. [49] Similarly, when it comes to advertising, every nanosecond of processing time between the user opening an online page and a customised advertisement popping up, makes a difference. It is in this context that blockchain technology would have to compete with providers such as Google in the field of customised advertisements, which can process 40 000 searches per second.[50]

That said, the trilemma is not an ironclad natural law like the speed of light. A number of new blockchain technologies are contributing to an overall solution.

---

[45] Kevin Werbach & Nicolas Cornell, 'Contracts Ex Machina' (n 142), available at https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3913&context=dlj (last accessed on 23 October 2019), p.335.

[46] Scalability, interoperability and sustainability of blockchain, a thematic report prepared by the European Union blockchain observatory and forum, available at https://www.eublockchainforum.eu/sites/default/files/reports/report_scalaibility_06_03_2019.pdf?width=1024&height=800&iframe=true, (last accessed on 23 October 2019).

[47] The World Payments Report 2018, https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/World-Payments-Report-WPR18-2018.pdf (last accessed on 23 October 2019).

[48] Visa Fact Sheet, https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf (last accessed on 23 October 2019).

[49] Osato Avan-Nomayo, 'Bitcoin transactions per second approaching all-time high' (21 February 2019), https://bitcoinist.com/bitcoin-transactions-per-second-approaching-all-time-high/ (last accessed on 17 December 2019).

[50] 'Google processes 40k searches per second', https://www.quora.com/Google-processes-40k-searches-per-second-On-average-a-web-server-can-handle-1000-requests-per-second-Does-that-mean-Google-can-run-using-only-40-web-servers (last accessed on 23 October 2019).

There are several ways in which this issue can be addressed, which are discussed below.

2.2.3.1. Number of transactions per block

One way of addressing the issue of transaction speed could be to increase the number of transactions which are held by each block in a blockchain. However, this would have a negative impact on decentralisation, as networks would become slower and more congested, transaction costs would go up, and the costs of running a full node would increase, as transactions would need more time to be processed. Consequently, the security and trustlessness of the system would be diminished.

2.2.3.2. Speed of adding blocks

The second option of addressing the issue of transaction speed would be to add more blocks to the blockchain quicker, reducing the block generation time by lessening the hash complexity. A disadvantage with regard to this option would be that as more blocks are involved in a transaction, more time will be taken up in order to verify such a transaction. Additionally, running more nodes would entail an increase in the costs.

The idea of increasing the speed with which blocks are added also relates to the question of whether a proof-of-work (PoW) and proof-of-stake (PoS) process is adhered to in order to achieve consensus about the validity of new blocks or transactions. The processing and validation on a blockchain according to an independent and competitive process includes the participation of numerous parties. Thus, the players who perform the validation should be rewarded and encouraged. PoW and PoS are basically the different approaches to deciding who gets the reward from mining.

Most open and permissionless blockchains and systems in cryptocurrency networks currently rely on a PoW validation process (Bitcoin and the Ethereum network both do, for example). Under this approach, a user is asked to solve complex computational puzzles. Once the user has successfully done so, the solution to this puzzle will be easy and quick to validate by other users, and if this occurs the transaction is validated and written into the blockchain (or a new block is created), and the miner is rewarded for solving the maths problem (e.g. in an amount of coins). Thus, under the PoW model, all parties are free to contribute to the processing power of the blockchain. However, a downside to this model is that it takes up a lot of electricity power.

However, PoS models can serve as alternatives. As part of this alternative, a user is asked to stake a certain amount of their tokens in order to have the chance of being selected to validate and process blocks of transactions. They are then randomly selected by the system and either receive a reward for carrying out the validation, or lose their stake for failing to do so. Therefore, the more tokens a user holds, the more power they will have to create additional next blocks. Since only one node is working on solving the computational mathematical problem, the energy use which is associated with this model is lower. On the other hand, this model has been said to enrich those who are already rich. The 'plutocracy effect' present in some staking systems can however be ameliorated by on-chain governance. If a community decides to do so it can implement rules which limit the amount of influence that very rich token holders. One way of doing this is by separating rules governing the economics of staking rewards from stake-based voting. Separate and nuanced systems can be set up to limit plutocracy and also to limit concentration of wealth. [51]

[51] Richard Red, 'What is on-chain cryptocurrency governance? Is it plutocratic?' (June 2018), https://medium.com/@richardred/what-is-on-chain-cryptocurrency-governance-is-it-plutocratic-bfb407ef6f1 (last accessed on 23 October 2019).

2.2.3.3. Sharding

A number of sharded blockchains are making significant progress on this issue. Sharding is a way of breaking one blockchain into many different blockchains for increased transaction throughout while maintain an overall ability to act as a state machine. The roadmap for Ethereum for instance indicates that sharding and a move to Proof of Stake are likely to occur in the next 18-24 months. Due to the fact that Ethereum secures a massive amount of value already the updates will be gradual and come as a series of tests running parallel to the network followed by an update of the software on the nodes. Similar solutions for scaling are also available on other blockchains. On Bitcoin for instance the lightning network allows network participants to open payment channels that are compatible with the Bitcoin network off-chain, execute any number of transactions at high speed and then eventually close the channel with its end state when it is no longer needed.[52]

2.2.3.4. New approaches to the Trilemma

In addition to investing significant resources in solving scalability and speed problems in currently deployed blockchains, there are a number of new network topologies and consensus algorithms that that have much higher performance without sacrificing security. One approach is the use of Directed Acyclic Graphs (DAG).[53] These are a type of distributed ledgers which operate without blocks. Notable among the DAG family is IOTA which was specifically developed for microtransactions and IoT applications.[54] In IOTA each new transaction is attached to two previous transactions, which it is said to *approve*. "Approving a transaction implies that its history was verified and found to be valid. In particular, it means all accounts have positive balances. This makes sure there are no double-spends or new illegitimate tokens created."[55] In practice this means that the network actually speeds up when it is under high load because the more transactions there are, the more verification of transactions takes place.[56]

Another important development in terms of efforts to scale blockchains is the use of verifiable delay functions (VDF).[57] VDFs "take a prescribed time to compute, even on a parallel computer, yet produce a unique output that can be efficiently and publicly verified." This provides an essential mathematical ingredient for consensus mechanisms which are much faster than the early PoS and PoW algorithms implemented in current version of Bitcoin or Ethereum for example.

Projects such Solana as are already achieving 50k transactions per second based on consensus mechanisms which centre around VDFs.[58] The theoretical upper bound for the Solana architecture is 710 thousand transactions per second (tps) on a standard gigabit network and 28.4 million tps on 40 gigabit network connection. Such efforts tend to be also based on Proof of Stake but there is no requirement for this. A VDF is not a consensus algorithm on its own but rather a mathematical building block around which such algorithms can be built. The key innovation within Solana is Proof of History (POH), a globally-available permissionless source of time in the network that works before

[52] Alyssa Hertig, 'Bitcoin's Dropping Lightning Capacity Might not Be a Bad Thing' (October 2019), https://www.coindesk.com/bitcoins-dropping-lightning-capacity-might-not-be-a-bad-thing (last accessed on 23 October 2019).
[53] 'An Introduction to DAGs and How They Differ From Blockchains' (June 2018), https://medium.com/fantomfoundation/an-introduction-to-dags-and-how-they-differ-from-blockchains-a6f703462090 (last accessed on 23 October 2019).
[54] https://www.iota.org
[55] Meet the Tangle, https://www.iota.org/research/meet-the-tangle (last accessed on 17 December 2019).
[56] Alon Gal, 'The Tangle: an illustrated Introduction' (Jan 2018), https://blog.iota.org/the-tangle-an-illustrated-introduction-4d5eae6fe8d4 (last accessed on 23 October 2019).
[57] VDF Research Effort, https://vdfresearch.org (last accessed on 17 December 2019).
[58] 'Solana: Web Scale Blockchain', https://solana.com (last accessed on 17 December 2019).

consensus. It layers a Practical Byzantine Fault Tolerance algorithm on top of this PoH clock to validate transactions.[59]

At the moment the live systems that are using PoS and more exotic consensus mechanisms and sharding are basically only useful for the most advanced users. The same thing applies to blockchains of blockchains like Polkadot and Cosmos. That said, technical advancement in the field is extremely fast and it should be expected that these technologies will progress to the level of user friendliness similar to Ethereum within 18-24 months.

2.2.4. Environmental concerns

In order to grasp the scale of the electricity power a blockchain system may require, one should note that running Bitcoin's software can take up almost as much power as the whole country of Denmark in terms of electricity consumption.[60] In early 2018, it was estimated that Bitcoin's proof-of-work consensus mechanism created yearly CO_2 emissions that could be compared to one million transatlantic flights.[61] As blockchain is expected to gain more and more popularity, its maintenance constitutes a huge environmental challenge. However, there are currently greener mining solutions being tested (e.g. Hydrominer). Moreover, there is a significant difference between countries in this regard; it costs more than $ 26 000 to mine just one Bitcoin in South Korea, one of the world's largest markets for cryptocurrency trading – whereas in Venezuela it costs just $ 531 to mine a Bitcoin.[62] Despite the fact that older blockchains such as Bitcoin will continue to be based on proof of work, most new blockchain development is occurring using Proof of Stake, variable delay functions and median timestamps.[63][64]

The issue in the future is likely to be less about whether new PoW systems will be built, but rather how to manage older decentralised systems outside the control of any one jurisdiction.

2.2.5. Cybersecurity

There is an ongoing debate about whether blockchain technology will serve as a help or a hindrance in terms of cybersecurity. On the one hand, blockchains can, for example, prevent data tampering and cyberattacks, and assist with identity and access management due to its encryption technology. On the other hand, cybersecurity practices, procedures and due diligence cannot be disregarded for blockchains and will have to be maintained in the same manner as with other cyber systems in order to not cause cybersecurity risks.

---

[59] Anatoly Yakovenko, '8 innovations that make Solana the First Web-Scale Blockchain' (July 2019), available at https://medium.com/solana-labs/7-innovations-that-make-solana-the-first-web-scale-blockchain-ddc50b1defda (last accessed on 17 December 2019).

[60] Mark Papermaster, 'Blokchains and Its Implementation Challenges' (April 2018), available at https://www.networkcomputing.com/network-security/blockchain-and-its-implementation-challenges (last accessed on 23 October 2019).

[61] Roman Beck, Christoph Müller-Bloch and John King, 'Governance in the Blockchain Economy: A Framework and Research Agenda' (2018), available at https://www.researchgate.net/publication/323689461_Governance_in_the_Blockchain_Economy_A_Framework_and_Research_Agenda, (last accessed on 23 October 2019), p.3

[62] Ryan Browne, 'It costs $26,000 to mine one bitcoin in South Korea-and just $530 in Venezuela' (Feb 2018), available at https://www.cnbc.com/2018/02/15/the-cheapest-and-most-expensive-countries-to-mine-bitcoin.html (last accessed on 23 October 2019).

[63] Anatoly Yakovenko, 'Proof of History: a clock for blockchain' (April 2018), available at https://medium.com/solana-labs/proof-of-history-a-clock-for-blockchain-cf47a61a9274 (last accessed on 23 October 2019).

[64] Hbar Economics, 'A deep dive into the dual rôle of Hbars and detailed release schedule', https://www.hedera.com/hh-hbar-coin-economics-paper-100919-v2.pdf (last accessed on 23 October 2019).

2.2.5.1. Cybersecurity opportunities; data tampering

Concerning the ways in which blockchain technology can contribute to cybersecurity, due to decentralisation, any blockchain system is resilient by nature. As data cannot be removed from a blockchain, changes or additions to data can be tracked and alterations of data can be detected at short notice (as they would have to be verified), and no data is stored centrally, blockchains make it more difficult to tamper with data. Moreover, as the blockchain grows in blocks, it becomes even more difficult to tamper with the data stored on them. More specifically, blockchain can help prevent access fraud and help safeguard identities – as instead of relying on a central authority (which due to their structure are easier to hack) to manage passwords, this data can be saved on the blockchain.

Additionally, due to the fact that the blockchain development community tends to be very privacy focused, there have been some excellent advances in so called systems with 'Privacy by Design'.[65]
Functionally this means that the systems in question severely limit the data which are written to the ledger and limit this data to only data which by design cannot be traced back to a user. Additionally, there is a movement toward systems providing 'self-sovereign identity' (SSI). This means essentially that individuals own their own identity data on their own devices and are empowered to selectively disclose aspects about their identity or offer cryptographic proofs about elements of that identity without making a wholesale disclosure of their data to a third party. Additionally, SSI enables people and machines to prove aspects about themselves without relying on contact with an issuing party. Furthermore, SSI enables the revocation of credentials should they expire or become invalid. This is a major contribution to cybersecurity as it may provide a secure identity layer which was missing in the development of the internet.[66]

Blockchain security measures vary with each application yet it could be said that they include in general:

- Transaction data integrity protection within blocks using cryptographic hashes;
- Public-private key method encryption to manage participant access.

Blockchain technology also chronologically records data blocks by securely tying each block to the previous and later blocks. This measure both prevents data tampering within a block because any attempt to alter the data changes the hash values, which other participants can rapidly detect; and provides the immutability principle widely touted for blockchain recorded transactions. Specific blockchain applications may use different security measures that affect risk levels. Potential users should investigate and understand the particular measures a blockchain application uses to avoid unexpected vulnerabilities. Private blockchains require heightened scrutiny because they may not have a robust network of users, which is essential for policing attempts to mistakenly or intentionally introduce erroneous data into a blockchain.[67]

It should be mentioned that PoS Systems are an alternative. They however rely on economic incentives models for security. Particularly in proof of stake systems, the more people who are invested in an honest economic outcome the more difficult it is to attack the system economically (i.e. by buying up enough assets or hash power to implement

[65] Privacy By Design, https://en.wikipedia.org/wiki/Privacy_by_design (last accessed on 17 December 2019).
[66] Andrew Tobyn, 'Sovrin ; What Goes on the Ledger?' (Sept 2018), available at https://www.evernym.com/wp-content/uploads/2017/07/What-Goes-On-The-Ledger.pdf.
[67] Jared R. Butcher, Steptoe & Johnson LLP, and Claire M. Blakey, Paul Hastings LLP, with Practical Law Data Privacy Advisor, Practical Law, 'Cybersecurity Tech Basics: Blockchain Technology Cyber Risks and Issues: Overview' (Jan 2019) , available at https://www.steptoe.com/images/content/1/8/v2/189187/Cybersecurity-Tech-Basics-Blockchain-Technology-Cyber-Risks-and.pdf (last accessed on 23 October 2019).

an attack). If the value of assets secured by the blockchain is smaller, it is easier to attack. For this reason, Bitcoin and Ethereum are considered to be more difficult to attack economically than say a new network like Cosmos. Also for this reason, there needs to be a legal space for such new networks to build economic value within a legal structure.

2.2.5.2. Cybersecurity opportunities; preventing cyberattacks

Blockchain technology can also help deter cyberattacks, as attacks will have to be aimed not at one centralised source of domain name systems – rather hackers would need to have access to multiple nodes in order to attack a system. Generally, each blockchain assumes that a certain proportion of the users of the system are dishonest / evil / colluding. Some level of resistance to this is built into the consensus algorithms. Typically, up to 33% of the nodes can be dishonest without breaking the system.[68]

Blockchain technology provides a stronger method than traditional, centralised computing services for securing a networked transaction ledger. For example, cyberattackers generally prefer to target centralised databases (and blockchains are usually decentralised) that once compromised infect and destabilise entire systems. Distributed ledger technologies increase cyber resiliency because there is no single point of failure. An attack on one or a small number of participants does not affect other nodes, which are able to maintain ledger integrity and availability; as well as continue transacting with each other. The enhanced transparency of distributed ledgers makes it more difficult for cyberattackers to corrupt blockchains using malware or manipulative actions. Each node holds an identical copy of the ledger so participants can quickly detect any attempt to corrupt or inappropriately modify the historical transaction record. The encryption technologies that blockchain applications use to build and link data blocks protect individual transactions and the entire ledger. Consensus mechanisms similarly protect new data blocks by requiring network participants to validate and continually compare them with past transactions, which makes it less likely for a cyberattacker or rogue organisation to inappropriately manipulate new ledger blocks.[69]

More likely attack vectors come from programming errors. Such errors can result in very significant economic losses. Even the best protocol programmers encounter such problems. The Zcash team for example, discovered and remediated a significant bug that could have enabled an attacker to double spend. They were able to catch the bug and patch it prior to it being exploited but it was a touch and go operation which they did secretly as part of a larger network upgrade.[70]

2.2.5.3. Cybersecurity opportunities; encryption technology

Using encryption keys in conjunction with PKI can provide organisations with a higher level of security. Encrypting data on a blockchain can provide organisations with a level of protection from a data confidentiality and data access control perspective. For instance, implementing secure communication protocols on blockchain (assuming the latest security standards and implementation guides), guarantees that even in a situation where an attacker tries to do a man-in-the-middle attack the attacker will not

[68] Dr. Arati Baliga, 'Understanding Blockchain Consensus Models' (April 2017), available at https://pdfs.semanticscholar.org/da8a/37b10bc1521a4d3de925d7ebc44bb606d740.pdf (last accessed on 23 October 2019).

[69] Jared R. Butcher, Steptoe & Johnson LLP, and Claire M. Blakey, Paul Hastings LLP, with Practical Law Data Privacy Advisor, Practical Law, 'Cybersecurity Tech Basics: Blockchain Technology Cyber Risks and Issues: Overview', available at https://www.steptoe.com/images/content/1/8/v2/189187/Cybersecurity-Tech-Basics-Blockchain-Technology-Cyber-Risks-and.pdf, (last accessed on 23 October 2019).

[70] Josh Swihart, Benjamin Winston and Sean Bowe, 'Zcash Counterfeiting Vulnerability Successfully Remediated' (Feb 2019), https://electriccoin.co/blog/zcash-counterfeiting-vulnerability-successfully-remediated/ (last accessed on 31 October 2019).

be able to either forge the interlocutor's identity or disclose any data while in transit. Even in an extreme situation scenario where long-term private keys are compromised, past sessions are kept confidential due to the perfect forward secrecy properties of security protocols.[71]

2.2.5.4. Cybersecurity risks

However, blockchains remain vulnerable to cyberattacks. With the increasing number of commercial transactions taking place with the use of digital technologies, and due to the fact that more and more personal and financial information is taking a digitised form, the risk of security breaches is constantly on the rise. Once smart contracts are employed, the whole transaction needs to be digitised. This means the sensitive information concerning the parties may not be adequately protected. For instance, in 2016, Bitcoin exchange platform 'Bitfinex' and cryptocurrency crowdfunding vehicle 'The DAO' were both hacked resulting in the funds being manipulated and stolen. At the same time however, smart contracts operate on a blockchain, which is generally either a shared public ledger or a private permissioned ledger. Therefore, it can provide some degree of security, as 'distributed ledgers are not vulnerable to a single point of failure. To be successful, a cyber-attack would need to not only infiltrate one user; it would have to attack multiple copies of the record held across the network'.[72] Blockchain, being a young and relatively untested technology, constitutes an attractive goal for hackers. Smart contracts have already been used for criminal purposes, which may pose more questions in relation to their dependability.[73] The increase in the value of cybercurrencies and in the use of smart contracts and blockchain technology have contributed to money laundering and theft, ransom demands, and illicit transactions (such as the Silk Road online marketplace saga where the site's owner was charged and convicted of numerous crimes including computer hacking and narcotics trafficking[74]).[75]

Blockchain applications are similar to other computer systems in the sense that the software coding errors can introduce cyber risks. Coding errors may be more likely to occur where network protocols implement unusual or new functionality for which potential vulnerabilities are not yet well understood. For example, in 2016, hackers exploited a coding defect in the source code of the Decentralised Autonomous Organisation (DAO),[76] a virtual organisation operated using smart contracts and built on the Ethereum public blockchain, resulting in the theft of Ethereum tokens valued in excess of $50 million at the time. Blockchain technology is also highly dependent on encryption algorithms. Commonly used encryption techniques are widely vetted and generally reliable. However, as computing techniques evolve, they may become more vulnerable to attack. Emerging technologies, especially quantum computing, which

[71] Deloitte, "Blockchain and Cybersecurity. Let's discuss", available at https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf, (last accessed on 23 October 2019).

[72] Allens, 'Blockchain reaction: understanding the opportunities and navigating the legal frameworks of distributed ledger technology and blockchain' available at https://www.allens.com.au/globalassets/pdfs/specials/blockchainreport.pdf (last accessed on 23 October 2019).

[73] Ari Juels, Ahmed Kosba, Elaine Shi, 'The Ring of Gyges: Using Smart Contracts for Crime' available at http://www.arijuels.com/wp-content/uploads/2013/09/Gyges.pdf (last accessed on 23 October 2019).

[74] James Martin, 'Lost on the Silk Road: Online drug distribution and the 'cryptomarket'' (October 2013) available at https://journals.sagepub.com/doi/abs/10.1177/1748895813505234 (last accessed on 23 October 2019).

[75] Mark Giancaspro, 'Is a "smart contract" really a smart idea? Insights from a legal perspective' (2017) n°33, Computer Law & Security Review, p.825.

[76] DAO is a complex combination of several smart contracts and DLTs. It can be defined as "innovative, software-controlled and unincorporated association, the aim of which is to pool their investor-members financial resources towards a common business perspective" (Filippo Annunziata, "Speak, if you can. What are you? An alternative approach to the qualification of tokens and Initial Coin Offerings", Bocconi Legal Studies Research Paper Series, February 2019, p.15.).

harnesses the unique properties of quantum particles to efficiently perform computing tasks, may make current encryption techniques much less secure.[77]

A cryptographic hash function is a special class of hash function that has certain properties which make it suitable for use in cryptography. It is a mathematical algorithm that maps data or arbitrary size to a bit string of a given size (a hash) and is designed to work in a one-way direction. By using anchor hashing, it is possible to access the immutable characteristics of blockchain mainnet in a future version of the solution developed. Due to the permissioned character of the blockchain, every participating party needs to trust the nodes. This means that a bad actor would have the chance to manipulate the seemingly immutable data as long as he runs a minimum of 51% of the nodes. This problem becomes less feasible the more nodes exist because a manipulation would need more actors involved trying to manipulate the data. For example, the Ethereum mainnet is very difficult to manipulate and due to its decentralisation it has the characteristics of an immutable database not found in private systems. Anchor hashing would provide an opportunity to detect manipulation in a private blockchain network. Intermittent snapshots of portions of the private blockchain transaction history could be hashed and written on the Ethereum mainnet. Later, if the transaction history of the private blockchain is in doubt, those portions could be hashed again and compared to the immutable mainnet records. If the result of this comparison is not identical then it could be inferred that manipulation occurred. Such mainnet snapshot capability could be built into future versions of this system and trigger an automated error or manipulation reporting mechanism.

Updateability is a bit of an issue here. The hashing techniques used in Bitcoin for instance are not generally seen as quantum computing resistant. If they cannot be upgraded prior to the advent of a practical quantum computer, the system may break. Bitcoin for instance uses a Hashing function from the MD5 family called SHA2. The previous versions of this hashing function were already broken (SHA0, SHA1).[78] We do not know how long it will take but there's a good likelihood that SHA2 will eventually also be broken and at the moment there is not a good way to upgrade the hashing function in Bitcoin's system. This results from the fact that Bitcoin was not designed with a governance system and suffers from significant defects in governance which do not permit the collaboration and alignment of incentives necessary for noncontentious software upgrades / forks. [79] Newer blockchain and DLT systems are generally implementing consensus mechanisms which are quantum resistant but upgradeability and governance remain the main issues overall. The latest generation of blockchains generally includes robust governance, upgradeability and interoperability between a number of different blockchains.[80]

[77] Jared R. Butcher, Steptoe & Johnson LLP, and Claire M. Blakey, Paul Hastings LLP, with Practical Law Data Privacy Advisor, Practical Law, 'Cybersecurity Tech Basics: Blockchain Technology Cyber Risks and Issues: Overview' , available at https://www.steptoe.com/images/content/1/8/v2/189187/Cybersecurity-Tech-Basics-Blockchain-Technology-Cyber-Risks-and.pdf, (last accessed on 23 October 2019).

[78] 'Security 'Secure Hashing: Approved Algorythms' https://web.archive.org/web/20110625054822/http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html (last accessed 24 October 2019).

[79] Aaron von Wirdum, 'A primer on Bitcoin Governance, or Why Developers Aren't in Charge of the Protocol', https://bitcoinmagazine.com/articles/a-primer-on-bitcoin-governance-or-why-developers-aren-t-in-charge-of-the-protocol-1473270427 (last accessed on 23 October 2019).

[80] Polkadot, 'Walkthrough of Polkadot's Governance' (July 2019), https://polkadot.network/a-walkthrough-of-polkadots-governance/; Jared R. Butcher, Steptoe & Johnson LLP, and Claire M. Blakey, Paul Hastings LLP, with Practical Law Data Privacy Advisor, Practical Law, 'Cybersecurity Tech Basics: Blockchain Technology Cyber Risks and Issues: Overview' , available at https://www.steptoe.com/images/content/1/8/v2/189187/Cybersecurity-Tech-Basics-Blockchain-Technology-Cyber-Risks-and.pdf, (last accessed on 23 October 2019).

Furthermore, some blockchains are susceptible to attacks of colluding selfish miners. Generally, nodes with over 51% computing power could reverse the blockchain and reverse the transaction that took place. However, recent research shows that even nodes with less than 51% power are still dangerous. In particular, the network is vulnerable even if only a small portion of the hashing power is used to cheat. In selfish mining strategy, selfish miners keep their mined blocks without broadcasting and the private branch would be revealed to the public only if some requirements are satisfied. As the private branch is longer than the current public chain, it would be admitted by all miners. Before the private blockchain publication, honest miners are wasting their resources on a useless branch while selfish miners are mining their private chain without competitors. So selfish miners tend to get more revenue. Rational miners would be attracted to join the selfish pool and the selfish could exceed 51% power quickly.[81] This problem is actively in discussion among Bitcoin miners where a concentration of hash power has undermined the decentralisation of the protocol.[8283] That said, technical advancements are leading toward a future where this problem will be solved – at least for protocols which have functional governance and can be upgraded. Pooled mining is for instance one feasible defence strategy. [84] Even for bitcoin there exist proposals for backwards compatible defences.[85]

2.3. Economic and governance context

2.3.1. Integration with legacy systems

The main consideration for companies to adopt blockchain technology is the hope that it will bring long-term benefits of productivity, efficiency and costs. However, there are often significant initial costs a company will have to incur as part of adopting this technology.

In order to make the change to a blockchain-based system, the organisation will have to either integrate their current systems with the blockchain or completely change their old system. Blockchain solutions will not match with all of the required capabilities of a particular organisation, meaning it cannot completely disperse of its legacy systems, and amendments will need to be made to the existing system – which will once again have implications in terms of resources.

Still, it is forecasted that worldwide spending on blockchain solutions will reach $11.7 billion in 2022.[86] Thus, there is an increased demand for enterprise blockchain.

2.3.2. Interoperability and standardisation

Blockchain-based platforms need to be able to communicate and share data. There are many ways to achieve interoperability between blockchains. These methods are

[81] 'Blockchain challenges and opportunities: A survey, International Journal of Web and grid Services' (October 2018), available at https://www.researchgate.net/publication/328338366_Blockchain_challenges_and_opportunities_A_survey/link/5bd1e50d299bf12253b018d9/download (last accessed on 23 October 2019).
[82] Kyle Torpey, 'Bitcoin Mining Centralization is 'Quite Alarming', But A solution is in the Works' (July 2019), https://www.forbes.com/sites/ktorpey/2019/07/28/bitcoin-mining-centralization-is-quite-alarming-but-a-solution-is-in-the-works/#25e5c6d1530b (last accessed on 23 October 2019).
[83] 'An Overview of Comos Hub Governance' (March 2019), https://blog.chorus.one/an-overview-of-cosmos-hub-governance/ (last accessed on 23 October 2019).
[84] Suhyeon Lee, Seungjoo Kim, ' Pooled Mining Makes Selfish Mining Tricky'(22 Dec 2018), available at https://eprint.iacr.org/2018/1230.pdf (last accessed 24 October 2019).
[85] Ren Zhang, Bart Preneel, 'Publish or Perish: A Backward-Compatible Defense against Selfish Mining in Bitcoin', KULeuven, available at https://www.esat.kuleuven.be/cosic/publications/article-2746.pdf (last accessed 24 October 2019).
[86] 'Worldwide Spending on Blockchain Forecast to Reach $11.7 Billion in 2022, According to New IDC Spending Guide' (July 2018), available at https://www.idc.com/getdoc.jsp?containerId=prUS44150518 (last accessed on 23 October 2019).

constantly being developed and improved, as interoperability is considered another key challenge in the blockchain world.

Despite the numerous enterprise blockchain platforms their capabilities are mostly being offered in isolation, without much overlap in what solutions they bring to their users, or sharing of data. These circumstances imply that there are obstacles to achieving inter-platform operation.

One of the obstacles in this regard is the choices different blockchains make in order to secure their safety. Whereas some blockchains might limit the number of participant nodes, for example, others might limit the design size of an application for interface with blockchain network and offline data storage.[87] These decisions are taken, and parameters are set, with the key capabilities offered by the blockchain or blockchain-based network in mind. For example, a network which offers payment services will need a different level and form of protection from one storing digital assets. These differences in approaches and priorities create obstacles for interoperability.

Moreover, coders and developers currently have total freedom when developing blockchain platforms. Consequently, there will also be differences in terms of coding, use of language and protocols, and consensus mechanisms among these platforms.

As of yet, only 25% of DLT platform operators have systems which are interoperable with other networks, and more than 50% of implemented solutions of technology by companies are based on an individual approach.[88]

Addressing and potentially solving this issue and having blockchain-based platforms work with each other and offer integrated capabilities as well as user-friendly experience to their users, is key in making a strong case for - and ensuring the mass adoption - of blockchain technology.

Part of the solution could be the setting of standards which could guide the implementation of blockchain solutions and allow different chains to interact with and recognise one another, as well as share information. Making blockchains interoperable in this manner would mean their uses would be significantly expanded as well. This, as the different blockchain platforms would create an ecosystem in which they can communicate easily without the need for an intermediary, and this would in turn allow for functionalities such as payments, data storing and smart contracts to co-exist as functionalities. However, so far there has been limited progress in this regard and blockchains continue to move into different directions from each other and offering different capabilities.

Much of the work at this point by the best protocol developers in the world is going into designing blockchains of blockchains with upgradeability and governance built in. There are two major networks which include support for many 'sub' blockchains which are interoperable with one another.[89][90]

[87] 'Can the interoperability of blockchains change the world?' (Feb 2019), https://www.capgemini.com/2019/02/can-the-interoperability-of-blockchains-change-the-world/ (last accessed on 23 October 2019).
[88] 'Efforts = effects? Blockchain standardisation overview', https://savangard.com/en/2018/08/22/blockchain-standardisation-efforts-overview/ (last accessed on 23 October 2019).
[89] https://polkadot.network (last accessed on 17 December 2019).
[90] https://cosmos.network (last accessed on 17 December 2019).

The EU Blockchain Observatory & Forum report[91] recommends that standardisation and interoperability are important for blockchains to work together and thereby for the ecosystem as a whole to benefit. Setting standards could help halt the fragmentation of the ecosystem. Moreover, they could facilitate an increased understanding of blockchain technology, which would extend the market, as well as promote competition. Standardisation could also help companies collaborate on development and solutions, and the validations of proofs of concept. That said, as a result of substantial efforts like Polkodot and Cosmos it may not be necessary for regulators to set standards centrally. What they can do is offer a place for experimentation where such tech can legally be tested live and gain the economic value necessary to secure large PoS systems. One example of such a system is the Kusama Canary net operated by Polkodot.[92]

The European Parliament noted that there is a 'constellation of DLT technologies with various technological characteristics as well as different mechanisms concerning governance (permissioned and permissionless distributed ledgers) and consensus.'[93] The efficiency needed for blockchain to evolve effectively requires ensuring efficiency requires interoperability between DLTs, between applications built on the same DLT, and between DLTs and legacy systems. Organisations such as ISO are already engaged in initiatives to develop standards for distributed ledger technology. It is important that such initiatives bear fruit.

It is also critical that there is a space for testing and scaling new networks with unknown topologies. Otherwise potential innovations will occur outside Europe and die on the vine here due to regulatory uncertainty.

2.3.3. Tokenisation as a means to provide incentives

Blockchains provide a new and unique opportunity to implement structures for incentivising human behaviour – a key part of economics – and thereby social outcomes. Tokenisation can incentivise certain specific behaviour by identifying the self-interest of each party involved, aligning each party's interest and identifying potential bad token behaviours. Distributed ledger technology can be used to reward good behaviour and disincentivise bad behaviour. The technology does so by establishing connections between different parties, and in a more traditional manner which involves centralised authorities designing these outcomes. However, a key condition for this opportunity is the assessment of how to provide incentives for encouraging behaviours which are in line with benefits and optimised functioning of the individual, organisations, the economy and the eco-system simultaneously.

Tokenisation offers a means to incentivise a network, by making participation independent of the goodwill of the actors. This principle can be extended to any area in which value can be generated through the coordination of peers; not just to services traditionally offered by private actors, but also to those provided by public actors. Examples include the cleaning up and maintaining of parks and neighbourhoods, care for elderly, as well as any other activities for which citizen engagement and participation may take over public policy. Tokenised incentive schemes thus have the potential to form incentives across a wide variety of economic actors who have some stake in the system. Tokens are programable and applicable in ways only limited by the imagination of programmers and the limits of regulation. A trivial example would for instance be a

[91] 'Scalability, interoperability and sustainability of blockchain', Op.Cit.
[92] 'Annoucing the Kusama Network' (July 2019), https://polkadot.network/kusama-network-the-canary-network/ (last accessed on 23 October 2019).
[93] European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation (2017/2772(RSP)), B8-0397/2018, available at https://www.europarl.europa.eu/doceo/document/B-8-2018-0397_EN.html (last accessed on 17 December 2019).

token whose value decreases if it is held too long. Actors could be thereby incentivised to actively use the token to purchase services as opposed to the unwanted behaviour of hoarding.

We already see similar systems in use which are not based on blockchain. The airline industry, in particular, has used centralised 'points-based' incentivisation systems for many years. The issue with those systems is, however, that they are closed centralised systems which do not allow transaction between various parties and thus have economic effects limited to the scope of their application.

Alternatively, incentivisation through tokenisation could be used and applied within an organisation. An example could be the awarding of tokens for completing a project based on the triggering of a smart contract when a task has been finished. Such a system would allow for the keeping of records of employees' projects and their dates of finalisation, and thereby the tracking of improvements, increased efficiency and a transparent workplace. Blockchain could therefore boost productivity by automating and reducing the burden of routine, data-heavy processes like VAT administration and payroll.[94] Furthermore, it could enhance fraud prevention and cybersecurity in HR.[95] Blockchain could also be useful in administering the office world, such as processing payments and creating audit records.[96]

2.3.4. Organisation and governance aspects

Blockchain governance is a polycentric process to which multiple actors contribute. There are various ways in which blockchains and blockchain-based applications can be governed. Determining the governance structure of a particular blockchain requires considering numerous elements, including the identities of the parties who can suggest changes, the ways in which these changes could be suggested, the identity of the parties who decide on protocol upgrades and those who implement the changes (such as coders, miners and coin holders).[97]

Blockchains generally have several layers. Each layer is part of a 'tech stack' contributing to the whole. Generally, as one advances up the tech stack, the level of abstraction increases. This means that at each successive layer, the underlying more basic functionalities or questions are taken as a given. This includes the governance of the underlying functionalities. The two obligatory layers include the network layer and the application layer. There might also be additional layers such as decentralised application layers or layers associated with scaling solutions or even interoperability.[98] There are numerous actors who contribute to the blockchain governance at each of these layers.

2.3.4.1. Centralised or decentralised governance

In the literature, blockchains are sometimes described as centralised or decentralised, and on-chain or off-chain. The first aspect (centralisation/decentralisation) describes the degree to which numerous actors are empowered to participate, particularly in the setting of rules for the blockchain system (algorithmic design for consensus, security model, governance model, etc.). Completely centralised blockchain systems exist and

[94] PwC, 'How blockchain technology could impact HR and the world of work', https://www.pwc.co.uk/issues/futuretax/how-blockchain-can-impact-hr-and-the-world-of-work.html, (last accessed on 23 October 2019).
[95] Ibidem.
[96] The Economist, '5 applications for blockchain in your business', https://execed.economist.com/blog/industry-trends/5-applications-blockchain-your-business (last accessed on 23 October 2019)..
[97] Michele Finck, Blockchain Regulation and Governance in Europe, Cambridge University Press (December 2018), p.185.
[98] Ibidem.

are well understood. In these blockchain systems, there exists some single point at which decisions can be made for the entire system. Blockchain systems can be decentralised by degrees but this decentralisation occurs along a continuum. On one pole is monolithic centralisation. On the other pole there is a nearly no theoretical limit to the level of decentralisation which one can imagine. In practice, however, most blockchain systems exhibit some level of centrality and some level of decentrality in terms of their power structures and governance. The level of decentrality can only really be expressed in relation to other systems which serve a similar purpose. In the context of governance, on chain / off chain refers to where decision-making and implementation occur. On-chain refers to informational processes which are modelled directly on the blockchain. Off-chain refers to decision-making and decision implementation processes that are not directly coded into the protocol of the blockchain in question.

Thus, it is established that blockchains can be more centralised or more decentralised. A more centralised blockchain is controlled by a determined party or an entity which whitelists nodes and determines the system's rules of operations. A blockchain is still considered to be more centralised even if the blockchain's nodes are located across the globe as long as it is centrally managed by a single entity.[99] An illustration of this principle could be a Google Doc: a document can be set up so that many persons may view or edit it, yet the infrastructure allowing the document to be created is maintained by a single company.[100] Examples of more centralised blockchains in today's world include the Linux Foundation's Hyperledger or the R3 Consortium's Corda.[101] Private permissioned blockchains are, however, not necessarily centralised by default. If they are administered by a wide range of actors who are themselves beholden to a decentralised governance process, they may indeed be fairly decentralised. An example of such a system is the Sovrin blockchain which is a fairly decentralised private permissioned chain, backed by an extensive off-chain governance system.[102] The question of centralisation is a question of power. When power within the blockchain is spread widely across many actors it may be considered decentralised to some degree. The degree of centralisation can be relatively independent of the security model of the blockchain.

Some blockchains have a higher level of decentralisation governance which allows the protocol to be modified in its initial deployment by users at various levels within the decentral tech stack. An example of a more decentralised blockchain could be DASH, which uses a consensus-based voting system to introduce changes to its protocol. Governance proposals within its network are submitted to stakeholders, who are in turn given a deadline to 'announce' their decision. Other examples include Tezos[103], Cosmos[104] and Polkodot[105], each of which has its own unique governance systems. Typically, these combine on-chain and off-chain elements and strive to solve problems not yet known at the time of initial system design by making the systems flexible and upgradeable.

Blockchain systems typically address the problem of decentral governance in part through cryptoeconomics: a combination of cryptography and economics. Crypto-economics focuses on the design of specific incentive structures which praise the

[99] Ibidem, p.195.
[100] Tatiana Cutts, 'Smart Contracts and Consumers', LSE Working Papers (Jan 2019), p.25.
[101] Op. Cit., M. Finck, p.195.
[102] 'Sovrin governance Framework', https://sovrin.org/stewards/, https://sovrin.org/library/sovrin-governance-framework/ (last accessed on 24 January 2020).
[103] 'Tezos', https://tezos.com/get-started/#governance (last accessed on 24 January 2020).
[104] Felix Lutsch,, 'An overview of Cosmos Hub Governance' (March 2019), https://blog.chorus.one/an-overview-of-cosmos-hub-governance/ (last accessed on 24 January 2020).
[105] 'A Walkthrough of Polkadot's Governance' (July 2019)https://polkadot.network/a-walkthrough-of-polkadots-governance/ (last accessed on 24 January 2020).

behaviour that enables the network to function properly, and discourages behaviour that leads to undesirable outcomes (e.g. network congestion, overuse, or other forms of abuse). Cryptoeconomic design involves a mixture of game theory, public choice theory, pure mathematics, economics, cooperative game theory and governance theory. Blockchain networks in-part operate via traditional market dynamics. This means they are, like laissez-faire economic systems, prone to oligopolistic outcomes in the absence of cryptoeconomic design or governance choices intended to mitigate the effects of or formation of cartels. The good news is that blockchains have programmable incentive structures and can integrate these into their governance. One specific example of this is ongoing in the Ethereum community. As part of the move to Proof of Stake, the Ethereum community is considering implementing a proof-of-stake protocol that is robust under cartel analysis. The details are beyond the scope of this discussion. However, the cryptoeconomic design takes into account the fact that cartels are likely to form and ensures that the network incentives of such cartels will be punished whenever validators appear to be missing (and censorship or an abuse of power has occurred).[106]

2.3.4.2. On-chain and off-chain governance

Blockchain governance processes comprise two dimensions: on-chain and off-chain. On-chain blockchain governance takes place directly on the blockchain protocol. Stakeholders make proposals and arrive at decisions through the protocol itself. A decision is reached on the blockchain (often via some form of voting). The effects of this on-chain governance could be varied depending on the area of the tech stack within which the governance takes place. Some governance processes are aimed at directly modifying or amending the underlying protocol. One example of a self-amending blockchain is Tezos, which implemented its update to the underlying network resulting in on-chain governance activity.[107] On-chain governance may also occur in the second or third layer portions of a blockchain ecosystem. Aragon is an example of this second layer governance. Aragon is an application layer governance framework built on top of Ethereum and enables the direct on-chain governance of entities operating on the Ethereum chain as opposed the governing of the underlying protocol itself.[108] On-chain and off-chain governance may be present in the same overall blockchain at the same time. Ethereum is largely governed at this time by an off-chain governance.[109] Despite this, it enables applications which have decentralised on-chain governance at their core (e.g. MakerDao[110], or Aragon[111]). Voting power in these systems differs according to system design. Some PoW systems essentially hand more power to groups of mining pools with more computing power (e.g. Bitcoin). Some PoS systems allow voting in proportion to the amount of native coins or tokens that the voter has. Some developing systems (including potentially Ethereum after it transitions to PoS in the next 12-18 months) rely on quadratic voting. Quadratic voting allows people to express how strongly they feel about an issue rather than just whether they are in favour of it or

[106] Vlad Zamfir, 'The History of Caser : Chapter 5'(Dec 2016), available at https://medium.com/@Vlad_Zamfir/the-history-of-casper-chapter-5-8652959cef58, https://blog.cosmos.network/consensus-compare-casper-vs-tendermint-6df154ad56ae. (last accessed on 24 January 2020).

[107] Jacob Arluck, 'Reflecting on Athens, the first self-amendment of Tezos' (May 2019), available at https://medium.com/tqtezos/reflecting-on-athens-the-first-self-amendment-of-tezos-4791ab3b1de1 (last accessed on 24 January 2020); Christine Kim 'Tezos Is About to Enact Its First-Ever On-Chain Blockchain Update' (May 2019), ,https://www.coindesk.com/tezos-is-about-to-enact-its-first-ever-on-chain-blockchain-update (last accessed on 24 January 2020).

[108] 'Governance', https://aragon.org/en/project/governance (last accessed on 24 January 2020).

[109] Bogdan Rancea, ' What is Ethereum Governance? Complete Beginner's Guide ' (Jan 2019), https://unblock.net/what-is-ethereum-governance/.(last accessed on 24 January 2020).

[110] 'Makerdao : A better money', https://makerdao.com/en/ (last accessed on 24 January 2020).

[111] ' Aragon', https://aragon.org/ (last accessed on 24 January 2020).

opposed to it. Furthermore, it imposes a quadratically increasing cost on allocating additional votes on any particular issue.[112]

2.3.4.3. Governance participation and models

Participation in voting processes for both on-chain and off-chain decisions can be incentivised by on-chain rewards, but this varies widely from project to project. At present there is no uniform best practice for effectively incentivising governance participation. This is especially true for getting the parties with the correct level of knowledge to participate at the level where they have the best understanding (i.e. users at the application layer, developers at the protocol layer, etc.)

Some on-chain governance systems suffer from low voter turn-out, especially if there is no optimal reward structure for the participants. In such cases, the issue is magnified by the risk of undemocratic voting. If some stakeholders in a PoS system choose not to vote, others with greater coin holdings will be able to determine the future course of the project. This is especially relevant, as often, the majority of coins are in the hands of the minority. Wealth is often (but not always) concentrated in a narrow number of stakeholders ('whales'). There is also the risk of the majority bias when the majority wins.[113] The system may potentially pave the way towards a pay-to-play decision making process whereby 'richer' stakeholders are able to eclipse their 'poorer' counterparty with sheer brute force.[114] Logically, however, this problem is dependent on the degree of decentralisation present in the system.

Off-chain systems of governance typically involve processes outside the blockchain or 'code' domain — only after having reached a decision, its implications are translated into on-chain action, such as for example a soft fork or investment allocation. Thus, this governance model makes use of pre-existing regulatory and compliance mechanisms to steer a blockchain network's future. For example, a management board is faced with a decision to introduce a new project feature and subsequently carries out an off-chain vote (in the physical space) with a certain result. That result, now documented manually, is imported onto the underlying blockchain infrastructure for execution—not much is done via technology here, aside from the execution phase. An off-chain governance involves a higher degree of human involvement and little use of code for decision making purposes. In the context of blockchain, this can help reduce code-based and data import mistakes. When taking on-chain decisions, one must be extremely careful not to write faulty code. Errors in the underlying protocol layer can result in unforeseen and unwanted economic outcomes. Blockchain's immutability increases the effects of human error. Off-chain governance models are thus somewhat helpful for mitigating this tendency. Similarly, there is something to be said for allowing decisions to be made by 'expert' opinions from the party holding the most information. Currently, Ethereum for example relies on a mostly off-chain governance method largely driven by a group of core developers who understand the underlying protocol code.[115]

Core Software Developers – in permissionless blockchains – coordinate through informal means and "exercise voice in proposing to project's architecture". There is no formal procedure for appointing and removing the Core System Developers, which underlines the informality of their function. At the same time, the Developers exercise significant

[112] Vitalik Buterin and Glen Weyl', 'Liberation Through Radical Decentralization'(May 2019), available at https://medium.com/@VitalikButerin/liberation-through-radical-decentralization-22fc4bedc2ac (last accessed on 26 January 2020).
[113] Ibidem, p.193.
[114] Op. Cit., Scalability, interoperability and sustainability of blockchain.
[115] 'Ethereum wiki '(April 2019), https://github.com/ethereum/wiki/wiki/Governance-compendium.(last accessed on 24 January 2020).

leverage over the systems by proposing solutions and structures to be applied.[116] The advantage of this arrangement is that the people best positioned to make the low-level protocol decisions have a large amount of influence in the community.

Off-chain governance may, however, logically be tied to transparency issues since it is generally driven by a smaller group of people. When decisions can be made behind closed doors and the network constituents are only able to see the output of those, one may logically question the validity behind decision-making processes. Coupled with having a select few (usually a type of a board) in charge of steering the course of a project, you arrive at the initial point of concern that leads to blockchain's development—stripping away central authorities and vesting power within the network and all its participants.[117] Foundation and association models are common vessels for the off-chain elements of governance that later flow into on-chain implementations. Most of the larger protocols (Tezos, Ethereum, etc.) have some kind of foundation which assists in governance at some level, with some level of transparency. These can either be transparent or non-transparent depending on their governance design and internally applied reporting requirements. As is the case with corporate governance and government, the transparency of the off-chain governance model is entirely dependent on design and intent.

As noted by the European Parliament, distributed ledger technology has the potential to decentralise governance and improve the capacity of citizens to hold governments accountable.[118] It could have a profound impact on the structure of public governance and the role of institutions. For example, unlike traditional currencies, cybercurrencies are not underpinned by any central banks. At the same time, there is a need to assess governance models within the diverse consensus mechanisms under development (especially including Proof of Stake), taking into account the potential needs of intermediary systems, actors and organisations in order to validate and verify the authenticity of the exchanges and to prevent fraudulent behaviour in good time.

2.4. Conclusion

This chapter has provided an overview of the technical, economic and governance context applicable to blockchain technology. Covering the most relevant aspects in this regard and outlining an understanding of the technology thereby sets the scene for the discussion and research to follow in the subsequent chapters.

[116] Op. Cit., M. Finck, p.200.
[117] Willem-Jan Smits, 'Blockchain governance: is it, what types are there and how does it work in practice', https://watsonlaw.nl/blockchain-governance-what-is-it-what-types-are-there-and-how-does-it-work-in-practice/, (last accessed on 23 October 2019).
[118] Ibidem.

3. Chapter 2 – Legal issues regarding blockchain technology

3.1. Introduction

This chapter sets out various legal issues relating to blockchain technology. We start by discussing the various general legal issues that have been noted in relation to this technology in general. However, considering that blockchain is a general-purpose technology and that as a consequence, legal and regulatory issues vary significantly depending on the specific use case, we also cover more specific legal issues on the basis of two broad use cases, namely smart contracts and utility tokens.[119] Building upon the technical, economic and governance context set out in the previous chapter, this chapter takes into account existing legal frameworks and assesses the relevance (including in terms of the risks and opportunities) of the legal issues presented.

3.2. Legal issues regarding blockchain technology

In this section, we introduce a number of general legal issues regarding blockchain technology that have been identified on the basis of our research.

3.2.1. Responsibility for legal compliance and liability

In decentralised networks, it can be burdensome to identify the actors responsible for legal compliance.[120] Indeed, whereas regulation has often been designed with centralised structures in mind (where responsibility for compliance can be allocated to an easy-to-identify legal person) the technical and organisational decentralisation of such structures can make it burdensome to allocate responsibility and compliance.[121] The degree of difficulty differs depending on whether the blockchain in question is permissioned[122] or permissionless.[123] Particularly public and permissionless blockchains are not governed by a single legal entity but rather by many loosely associated individuals based in various jurisdictions.[124] Much supranational legislation was adopted in the pre-digitalisation era or with online platforms controlled by a single legal person in mind and often focus on the territoriality principle. Where a global network is controlled by a centralised legal entity (such as an online intermediary platform) this is not necessarily a problem. Identifying a regulatory access point is, however, more complicated where there is no centralised legal entity responsible for the network. Determining the most suitable regulatory access points in decentralised networks is thus

[119] Both smart contracts and utility tokens are defined as "broad use cases" in Chapters 2-4, since the legal analysis does not require an in-depth assessment of more specific use cases.
[120] Michèle Finck, Blockchain Regulation and Governance in Europe, Cambridge University Press, 2019, Chapter 2.
[121] For an example from data protection law, see 'Data subjects as data controllers: a Fashion(able) concept?' (June 2019), https://policyreview.info/articles/news/data-subjects-data-controllers-fashionable-concept/1400 (last accessed on 17 December 2019).
[122] "A blockchain is permissioned where its participants are preselected or subject to gated entry on satisfaction of certain requirements (this could include, for example, a requirement that a participant must first satisfy KYC and AML requirements) or on approval by an administrator of the blockchain. A permissioned blockchain may use a consensus protocol for determining what the current state of a blockchain should be, or it may use an administrator or sub-group of participants to do so." Norton Rose Fulbright, 'Unlocking the blockchain. A global legal and regulatory guide. Chapter 1: An introduction to blockchain technologies', p.20.
[123] "A blockchain is permissionless when anyone is free to download the software, submit messages for processing and/ or be involved in the process of authentication, verification and reaching consensus. While a permissionless blockchain will typically use a consensus protocol for determining what the current state of a blockchain should be, it could also use some other process (such as using an administrator or sub-group of participants) to determine that state. Such systems are typically controlled by no-one and the participants are usually pseudonymous. Norton Rose Fulbright, 'Unlocking the blockchain. A global legal and regulatory guide. Chapter 1: An introduction to blockchain technologies', p.20.
[124] Ibid, Chapter 7.

an important question.[125] Indeed, stakeholders seem to consider that these questions are among the most important regulatory issues to have emerged in relation to blockchain to date.[126] Others have, however, also rightly stressed that while every blockchain system is unique, many of them are run exclusively by a single legal entity, in which case many of these issues do not arise.[127]

These circumstances also generate problems in relation to liability. Computer code does not always execute as planned, such as where there is a bug in the code.[128] This opens up the question of which actor should be liable in such an instance (such as the programmer, the party for whom the programmer worked, or the platform that provided the smart contract functionality).[129] Stakeholders consider that there is no legal clarity in relation to this issue.[130] In fact, the lack of a suitable legal framework that would determine the rights and obligations of each party and especially the lack of clear rules on liability has been criticised in the European Banking Authority's opinions of 2013, 2014 and 2016. It has been identified as a risk by consumers in transactions related to services provided by the crypto-assets trading platforms (note, though that such platforms are actors that can be easily identified).[131] Some sources underline that in an open source model, liability is not necessarily inherent (unlike in the proprietary model) and limitations of liability in open source models are often expected.[132] At the same time, if open source developers were not allowed to disclaim liability, the costs of code development could rise significantly, as they would need to account for any possible legal costs and may be discouraged from developing new software due to fears of possible liability.[133] Therefore, software developers and public blockchain advocates repeatedly note that public blockchain software is issued under the open source software licenses, which generally disclaim liability for any claims arising from the software.[134] Nevertheless, the liability of software developers of public blockchain systems has been examined in the relevant literature on multiple occasions.[135] Moreover, the legal literature has amply stressed that decentralisation narratives ought to be questioned as oftentimes the 'veil of decentralisation' is invoked by those wanting to shield themselves from liability for operating a non-compliant system.[136] This, of course, is undesirable and the effective enforcement of existing norms at national and supranational levels forms an important key to counteracting this.

A relevant question is moreover that of the standards of liability (such as negligence, strict liability etc) that should apply. It has been argued that an accountability standard

[125] See also Primavera De Filippi and Aaron Wright, Blockchain and the Law, Harvard University Press, 2018, Part 5.
[126] Interview with Chaineum, The Marshall Plan Holding, Norwegian Consumer Council, Gide Loyrette Nouel, Danish Consumer Council.
[127] Based on feedback received during the workshop (more information on the workshop can be found in the introduction of this report).
[128] At the workshop, it was however noted that a smart contract can be simulated before execution (more information on the workshop can be found in the introduction of this report).
[129] Angela Walch,' In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains' (2018), in Georgios Dimitropoulos et al (eds), *The Blockchain Revolution: Legal & Policy Challenges*, Oxford University Press, 2018.
[130] Interview with Nina Siedler.
[131] European Banking Authority, Report with advice for the European Commission on cryptoassets (January 2019), available at https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf, (last accessed on 23 October 2019).
[132] Kirk St Amant, 'Research Handbook on Open Source Software', Hershey, 2007, p.333.
[133] Kirk St Amant, Research Handbook on Open Source Software, Hershey, 2007, p.334.
[134] Ibidem, p.21.
[135] Tim Swanson, 'Who are the Administrators of Blockchains?' (October 2017), available at https://www.ofnumbers.com/2017/10/19/who-are-the-administrators-of-blockchains/ (last accessed on 23 October 2019).
[136] Angela Walch, 'Deconstructing 'Decentralization: Exploring the core Claim of Crypto Systems' (Feb 2019), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3326244 (last accessed on 23 October 2019).

proportionate to the seriousness of the services of the provider would benefit the users.[137] To address these issues, there are now ongoing efforts in the context of the International Standards Organisation[138] as well as existing principles and recommendations coming from open source software.[139] The literature suggests that two types of liability could arise here: strict liability for any fault in a product/for negligence or a reasonable-care standard. Under a strict liability standard, manufacturers and coders would be liable for any defect in the code that is executed to make their system function. This would create the expectation of perfection on the side of the coder. As a result the costs to coders/producers/manufacturers would be so high that innovation would not be sound from a financial viewpoint, hence it is possible that any blockchain development would be disincentivised. [140] These questions of liability closely relate to the point that has been made in relation to decentralisation above as most legal frameworks were adopted for centralised structures and it is accordingly often unclear how these ought to be matched to decentralised structures.[141] A limited liability approach for developers similar to that of companies could help to safeguard and promote innovation and risk-taking. Hence, a liability standard focussing on reasonableness and best efforts in order not to make the costs for the innovation too severe might eventually be developed by the legislature. For instance, it may be expected that industry will do its best to ensure the systems on products are secure against cyberintrusions, yet perfection as such will not be expected.[142]

It is accordingly apparent that many elements of liability have been discussed in relation to blockchains. On the one hand, some have worried about the practical enforcement of existing law to hold those breaking the law liable. It was stressed that enforcing existing law in relation to crypto projects has been a challenge in the past although many now appear to consider that more sustainable projects are taking over. [143] Moreover, it has been rightly argued that Member States have measures to tackle liability issues (think of criminal law enforcement) and classic remedy systems could apply also in this context.[144] Others have stressed that liability may be an issue in that it can be difficult to identify actors liable for compliance in contexts of decentralisation. Yet, the management of this difficulty is essentially a governance question – meaning that the relevant governance structure should be designed to accommodate for legal requirements.[145] Stakeholders have moreover suggested that this could also be simplified through standard terms and conditions as well as model contracts.[146] It has been pointed out that even where this is not the case, law enforcement agencies will

[137] Angela Walch, 'In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains' (2018), in Georgios Dimitropoulos et al (eds) *The Blockchain Revolution: Legal & Policy Challenges*, Oxford University Press, p.17.
[138] ISO/TC 307 is preparing standards on this matter, https://www.iso.org/committee/6266604.html (last accessed on 17 December 2019).
[139] See, by way of example: Kirk St Amant, Research Handbook on Open Source Software (2007), Hershey.
[140] Paul Rosenzweig, 'Bad Code Is Already a Problem. Soon, Companies Will Be Liable' (July 2017), available at https://foreignpolicy.com/2017/07/28/bad-code-is-already-a-problem-soon-companies-will-be-liable/ (last accessed on 23 October 2019).
[141] Interview with John Salmon.
[142] Paul Rosenzweig, 'Bad Code Is Already a Problem. Soon, Companies Will Be Liable' (July 2017), available at https://foreignpolicy.com/2017/07/28/bad-code-is-already-a-problem-soon-companies-will-be-liable/ (last accessed on 23 October 2019).
[143] Interview with the German Federal Financial Supervisory Authority (BaFin).
[144] Based on feedback received during the workshop (more information on the workshop can be found in the introduction of this report).
[145] Based on feedback received during the workshop (more information on the workshop can be found in the introduction of this report), Interview with Nina Siedler.
[146] Based on feedback received during the workshop (more information on the workshop can be found in the introduction of this report).

find access points to enforce regulation.[147] Depending on the specific area at stake, access points for attributing liability (such as in the form of a damage claim) and compliance may be the same or different actors, depending on the specific circumstances at stake and area of the law concerned. It must be stressed that even where no suitable governance arrangements exist, law enforcement agencies may bring claims against actors that participate in the administration of the given blockchain use-case, such as for instance miners, nodes, core developers, Internet Service Providers or even users.[148]

The amendment of on-chain code requires an offline coordination process by human beings and this coordination is likely to have legal consequences. For instance, in Germany, collaboration around a mutual goal is likely to give rise to the legal structure of the civil law partnership with unlimited legal liability for all partners.[149] This can be understood as a powerful incentive for blockchain-users to take governance arrangements seriously.

3.2.2. Potential barriers in sectoral (e.g. AML) legislation

Potential barriers in sectoral legislation that may prevent blockchains from unleashing their socio-economic potential in the EU have been discussed in recent years. Whereas not all sectoral legislation can be highlighted here, we focus on those areas the discussion has been centred on. Of course, depending on the use case, any area of EU law can become relevant for blockchains. For instance, one of our interview partners considered that the most important legal issues in respect to DLT relate to competition law, IP law such as trade secrets, yet also that the resulting legal questions are not specific to blockchains.[150] A similar point was made in relation to questions regarding the transfer of ownership.[151]

Much has been said in relation to blockchains' relation to the General Data Protection Regulation ('GDPR') and interview partners also stressed difficulties in relation to the application of the GDPR to blockchains and the need for solutions in this respect.[152] Notwithstanding, considering that the tension between the technology and the legal framework have been amply noted elsewhere such as in a recent study for the European Parliament this topic is not examined here.[153] Moreover, the European Data Protection Board is already looking into this issue.[154]

Data localisation requirements and data retention rules are also important regarding blockchain technology. Indeed, as blockchains are a form of database, all EU regulation on the treatment of data is particularly important in their respect. On the one hand, data localisation requirements may be difficult to abide by in relation to transnational data networks. The EU has, however, already taken important action in this respect as the new Regulation on the Free Flow of Non-Personal Data seeks to ensure the free

[147] Primavera De Filippi, Aaron Wright, 'Blockchain and The Law: The Rule of Code', Harvard University Press (March 2019), available at https://www.hup.harvard.edu/catalog.php?isbn=9780674241596&content=toc, Chapter V. (last accessed on 17 December 2019).
[148] Ibidem.
[149] Interview with Nina Siedler.
[150] Interview with the Blockchain Alliance.
[151] Interview with Consensys.
[152] Interview with the Swiss Cryptovalley Association; Interview with Nina Siedler.
[153] See, e.g. 'Blockchain and the General Data Protection Regulation' (July 2019), https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2019)634445 (last accessed on 23 October 2019).
[154] EDPB Work Program 2019/2020 (Feb 2019), https://edpb.europa.eu/our-work-tools/our-documents/work-program/edpb-work-program-20192020_en (last accessed on 23 October 2019).

movement of data in the internal market, which is a technology-neutral legal framework that also applies to DLT.[155]

Data retention rules, such as those arising under the Anti Money-Laundering Directive require that customer identity documents and transaction records be stored for five years after the end of the business relationship with the customer.[156] This in itself does not appear difficult in relation to blockchains, as indeed one of their features is that data can be stored for a long time period in a tamper-resistant manner.

Know-Your-Customer (KYC) processes are critical in order for financial institutions to comply with anti-money laundering efforts. In order to comply with KYC guidelines, a financial institution is required to collect, track and store all relevant customer data in case it needs to be reported to a regulatory agency. A KYC process is initiated whenever a customer requests to work with a financial institution in any capacity. Generally, the process commences with the customer sending certain original documents to the financial institution, and involves these documents being analysed and verified by the institution, background checks being carried out, and the identity of a person being verified. This process is also applied to any relevant subsidiaries and will need to be repeated for every collaboration between a customer and a financial institution.[157]

It has been argued that the costs, efforts and paperwork involved in KYC processes constitute a huge challenge for the financial sector.[158] A 2017 Thomson Reuters survey on the impact of global changes in KYC regulation on corporates, for example, found that on average it takes 32 days to complete KYC checks, and financial firms hired – on average – 307 new employees in 2017 to deal with these regulations.[159] Moreover, some firms are heavily fined for not complying with KYC regulations.[160] Lastly, there are the indirect costs incurred by the fact that financial institutions are barred from conducting business with parties for which the KYC process has not yet been successfully completed, and the delay this causes in the business relationship for both sides.[161]

Under the current system, each institution carries out required KYC checks separately and individually. For example, each bank will carry out an identity check for customers

[155] 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, COM (2017) 495. See also *"Cross-border data flow in the digital single market" (2017)*, by time.lex, Spark Legal Network and Tech4i2, available at https://op.europa.eu/en/publication-detail/-/publication/b23dc977-9e77-11e7-b92d-01aa75ed71a1 (last accessed on 17 December 2019).

[156] Articles 40(1)(a) and (b) 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 L 141, 73-117.

[157] Jose Parra-Moyano, Omri Ross, 'KYC Optimization Using Distributed Ledger Technology' (Jan 2017), available at https://www.researchgate.net/publication/315046134_KYC_Optimization_Using_Distributed_Ledger_Technology (last accessed on 23 October 2019).

[158] 'Using blockchain for KYC/AML compliance' (May 2019), https://www.dentons.com/en/insights/articles/2019/may/28/using-blockchain-for-kyc-aml-compliance (last accessed on 23 October 2019).

[159] 'KYC Compliance: the rising challenge for corporates', https://www.refinitiv.com/content/dam/marketing/en_us/documents/reports/kyc-compliance-the-rising-challenge-for-corporates-special-report.pdf. (last accessed on 23 October 2019).

[160] 'U.S., EU fines on banks misconduct to top $400 billion by 2020-report' (Sept 2017), https://in.reuters.com/article/banks-regulator-fines/u-s-eu-fines-on-banks-misconduct-to-top-400-billion-by-2020-report-idINKCN1C210D. (last accessed on 23 October 2019).

[161] Jose Parra-Moyano, Omri Ross, 'KYC Optimization Using Distributed Ledger Technology' (Jan 2017), available at https://www.researchgate.net/publication/315046134_KYC_Optimization_Using_Distributed_Ledger_Technology (last accessed on 23 October 2019).

taking out an online loan, starting from scratch for each check. Logically, this leads to inefficiencies. Moreover, the relevant data is collected and exchanged among organisations, businesses and institutions which each have their own protocols and processes. This lack of transparency has led to even greater inefficiencies in the collating of data.[162] Additionally, there are security risks, inaccuracies and errors involved in every check (simply due to the fact that data is being transmitted on a daily basis among these different actors).[163]

Some consider that blockchains may provide functionality for the 'passporting' of identity for KYC, AML or other client onboarding purposes.[164] This highlights how blockchains may be used as a 'regulatory tool' (that is to say a technical tool that facilitates regulatory compliance) in line with the recent recommendations of the EU Blockchain Observatory and Forum.[165] Blockchain technology is said to facilitate the streamlining of KYC processes in the financial services industry, as it allows for the accumulation and storage of data on client transaction activity history from multiple service providers. The technology can thus foster easier, faster and safer processes compared to those currently in place, as various service providers would be able collect information into a single database, such as for instance a blockchain or other solutions, ensuring coordination and avoiding duplications of effort. [166] Of course, the performance impact of additional data shared needs to be accounted for in any cost-benefit analysis regarding the suitability of such solutions as well as the usefulness of blockchains compared to other databases. One idea is that the financial services sector could implement the blockchain, and government institutions and companies could in turn rely on the data stored on it.[167] In this scenario, the need for another validation process or cross-checking of the data could be removed.[168] The improved relationship between financial institutions and regulators and the fact that governmental actors would be able to have improved access to data, could prove beneficial in terms of fighting and preventing fraud. [169] Lastly, utilising a shared database such as blockchain could mean that the costs associated with KYC guidelines could be shared proportionally among the relevant financial institutions, for example per customer.[170] It has, however, been stressed that these benefits can only be realised through private blockchains as compliance with KYC rules has proven difficult in the case of permissionless blockchains.[171]

---

[162] 'Why is Blockchain A Good Solution for KYC Verification', https://www.devteam.space/blog/why-is-blockchain-a-good-solution-for-kyc-verification/ (last accessed on 23 October 2019).
[163] Rakesh Sharma, 'Why a New 'Know you Customer' Project is Crucial to Blockchain' (June 2019), available at https://www.investopedia.com/news/why-new-know-your-customer-project-crucial-blockchain/ (last accessed on 23 October 2019).
[164] 'Unlocking the blockchain: a global legal and regulatory guide', https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/imported/unlocking-the-blockchain---chapter-1.pdf. (last accessed on 23 October 2019), p.23.
[165] EU Blockchain Forum and Observatory, 'Report on Legal and Regulatory Framework for Blockchains and Smart Contract's, available at https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf?width=1024&height=800&iframe=true (last accessed on 23 October 2019). p.21.
[166] Op. Cit., Rakesh Sharma, 'Why a New 'Know you Customer' Project is Crucial to Blockchain' (June 2019) available at https://www.investopedia.com/news/why-new-know-your-customer-project-crucial-blockchain/ (last accessed on 23 October 2019).
[167] Bryan Weinberg, 'Blockchain and KYC: Know Your Customer Better' (Jan 2019), https://openledger.info/insights/blockchain-kyc/ (last accessed on 23 October 2019).
[168] Op. Cit., 'Why is Blockchain A Good Solution for KYC Verification', https://www.devteam.space/blog/why-is-blockchain-a-good-solution-for-kyc-verification/ (last accessed on 23 October 2019).
[169] Ibidem.
[170] Jose Parra-Moyano, Omri Ross, 'KYC Optimization Using Distributed Ledger Technology' (Jan 2017), available at https://www.researchgate.net/publication/315046134_KYC_Optimization_Using_Distributed_Ledger_Technology (last accessed on 23 October 2019).
[171] Based on feedback received during the workshop (more information on the workshop can be found in the introduction of this report).

From the point of view of the customer, having such a system in place would mean they would only have to complete the KYC check once and after this use a database or platform could also be used to confirm the customer's identity. Access to their data would be provided to parties with the appropriate permission, and the customer would be able to maintain direct oversight as data 'owners' would still be required to authorise a party to access their data.[172] Additionally, in terms of the customer experience, involving blockchain technology into the KYC processes could mean shorter waiting times. In 2017, the Infocomm Media Development Authority of Singapore collaborated with a number of major banks in order to complete a 'proof-of-concept' for a KYC blockchain.[173] The prototype successfully passed the Monetary Authority of Singapore's test scenarios.[174] The results of this prototype illustrated that this specific blockchain solution functioned well despite high-volume information flows. The results also showed that this blockchain remained tamper resistant to third-party intervention while at the same time securing confidentiality by only allowing access to those with authentication.[175] The outcome of the prototype testing have been described as delivering assuring results on its functionality, scalability, and security.[176] Overall, it has been estimated that the use of a blockchain platform could result in cost savings of 25-50 percent by reducing duplication and providing a clear audit trail.[177]

SSI systems may be a blockchain-based solution for these inefficiencies. SSI systems are designed based on the principles of privacy-by-design and allow users to prove aspects about themselves while only disclosing identity information selectively. The verifiable credentials issued by such systems are also revocable. One could well imagine a situation where once a customer has passed KYC / AML with one provider they could use the credentials received in that transaction to streamline all future transactions. That said there are some issues with uniting eIDAS with SSI. The eIDAS was built with hierarchical trust centres and trust schemas in mind. Indeed, the bulk of the eIDAS legislation was passed before there was any discussion about blockchains or SSI.

Additionally, blockchains and smart contracts as such do usually have a technical link to any of the traditional eIDAS systems. 'Message Signatures' within the context of smart contracts and 'signed' transactions are the result of public-key cryptography. This cryptography underpins a huge portion of the modern economy and is the backbone mathematics that enables for example, ssl, tls and rsa. Indeed, HTTPS is also based on public-key cryptography. Moreover, this type of cryptography underpins eIDAS qualified digital certificates issued by qualified trust service providers.

The critical difference between this process and that employed in most blockchain contexts is that the process for creating a qualified electronic signature is highly permissioned and based on the aforementioned hierarchical trust model. It is also called public key infrastructure. In this model, one has to trust the 'trusted list'. If that list is trustworthy, one can verify the source, authenticity, integrity and validity of any data

[172] Olga Stashenko, 'Blockchain for know your customer (KYC): use cases' https://merehead.com/blog/blockchain-for-know-your-customer-kyc-use-cases/ (last accessed on 23 October 2019).
[173] Samburaj Das, 'Singapore Regulator, Bank Complete KYC Blockchain Prototype' https://www.ccn.com/singapore-regulator-banks-complete-kyc-blockchain-prototype/ (last accessed on 23 october 2019).
[174] 'Blockchain KYC utility', https://home.kpmg/xx/en/home/insights/2018/02/blockchain-kyc-utility-fs.html, (last accessed on 17 December 2019).
[175] Samburaj Das, 'Singapore Regulator, Bank Complete KYC Blockchain Prototype' https://www.ccn.com/singapore-regulator-banks-complete-kyc-blockchain-prototype/ (last accessed on 23 october 2019).
[176] 'The KYC Blockchain Breakthrough'(Feb 2019), https://www.asiablockchainreview.com/the-kyc-blockchain-breakthrough, (last accessed on 17 December 2019).
[177] 'Blockchain KYC utility', https://home.kpmg/xx/en/home/insights/2018/02/blockchain-kyc-utility-fs.html, last accessed on 17 December 2019).

contained in the qualified electronic signature. The Achilles' heel of the system is, however, that if the certificate authority or root trust service provider is compromised, the entire system falls apart. This has happened a number of times already.[178]

eIDAS systems try to provide the following characteristics:

- Credentials have not been tampered with
- Credentials are still within their validity period
- Credentials have not been revoked by the issuer
- Credentials have the intended semantics
- Credentials have been provided by a trustworthy issuer

Public blockchains, in contrast, are permissionless. A blockchain signature on an Ethereum smart contract for instance only verifies the authentication and integrity of the message. At the protocol level, these systems do not attempt to verify whether the actor signing a transaction can be trusted. They only check whether the message signed meets the qualifications for a valid signature.

This design is intentional. The designers of public blockchains are attempting to build trustless systems that enable users to interact as though they were able to trust one another (even though they do not/cannot). This works by combining public-key cryptography with a distributed probabalistic clock PoW or in the case of PoS (randomly distributed) authority backed by complex automated incentives models.[179][180]

With that in mind, the question is whether a blockchain could fulfil the requirements laid out under eIDAS while maintaining at least in large part the desirable traits of permissionlessness, decentrality and trustlessness at the network level. SSI systems attempt to solve this issue. Currently, however, there no SSI providers that attempt to produce a blockchain-based eSignature compliant with eIDAS. One example of a blockchain company which attempts to do something closely related though is SelfKey.[181]

In contrast, it has also been noted that using a distributed ledger may make it more difficult to adhere to existing AML regulations. This is problematic, particularly also since EU law makes it clear that these rules need to be applied in a technologically-neutral manner. Indeed, the 5th AML Directive mandates that related rules apply to wallet providers and cryptoasset exchanges. Nonetheless, it is well-known that some cryptocurrencies have been used for illicit purposes including money-laundering.[182] Moreover, terrorist groups have experimented with blockchain-based cryptocurrencies as a means of managing their financing.[183] These risks as well as the related legal obligations under the AML Directive underline that existing rules must be effectively

[178] Roel Schouwenberg, 'Why Diginotar may turn out more important than Stuxnet' (Sept 2011), https://securelist.com/why-diginotar-may-turn-out-more-important-than-stuxnet/30826/ (last accessed on 17 December 2019).
[179] 'Blockchain Proof-of-Work is a Decentralized Clock' (Jan 2018), (https://grisha.org/blog/2018/01/23/explaining-proof-of-work/) (last accessed on 17 December 2019).
[180] Aparna Krishnan, 'Randomness in Blockchain Part 1' (Sept 2018), available at (https://medium.com/mechanism-labs/randomness-in-blockchains-part-1-79192b173816) (last accessed on 17 December 2019).
[181] Martin Schäffner, 'Master's Thesis - Analysis and Evaluation of Self-Sovereign Identity Systems' (Nov 2019), available at https://github.com/Bartkeeper/thesis (last accessed on 17 December 2019).
[182] Tom Robinson, D.Phil & Yaya Fanusie, 'Bitcoin Laudering: An Analysis of Illicit Flows into Digital Currency Services', available at https://info.elliptic.co/whitepaper-fdd-bitcoin-laundering (last accessed on 23 October 2019).
[183] Allen & Overy, 'Legal and Regulatory risks for the finance sector: Cryptocurrency AML risk considerations', http://www.allenovery.com/publications/en-gb/lrrfs/cross-border/Pages/Cryptocurrency-AML-risk-considerations.aspx (last accessed on 23 October 2019).

complied with when DLT is used. Sometimes, particularly in relation to public and permissionless systems, this can be hard to operationalise in practice. Indeed, in some systems such as Bitcoin or Monero, no governance structures exist that enable compliance with these, and other rules. Furthermore, it has been noted that many companies subject to KYC rules are unaware that these rules apply to them, which is reflected by their design choices.[184] Nonetheless, this does not relate to the technology per se but rather to the governance structures around it as blockchains can indeed be used in a manner that allows compliance with existing regulations.[185] Essentially, these issues can thus be solved through governance decisions and the effective enforcement of existing law.[186] Some stakeholders have noted that with time, business models will move in a direction more facilitative of compliance with KYC requirements.[187] National regulators such as the Swiss FINMA have now taken steps in that direction.[188] It is also worth noting that some consider that AML legislation does not apply to pure utility tokens as here the main rationale is to provide access to a non-financial application.[189]

3.2.3. The protection of fundamental legal principles and mandatory rules

DLT's tamper-evident nature entails that data cannot easily be changed. Conversely, DLT can also be used to infringe fundamental legal principles or mandatory rules (such as the prohibition of child abuse materials, drug trafficking or money laundering) and it can be difficult to remove related content from the database.[190]

A European Parliament study recently highlighted that the anonymity and cross-border nature of such networks as well as the lack of central intermediary create challenges regarding law enforcement.[191] However, the resulting issues are not necessarily unique to blockchains. Indeed, other technical and non-technical tools can be relied on to facilitate similar behaviour. Blockchains are not necessarily more likely to be used for criminal activity compared to other solutions. For example, cash still remains the predominant instrument of money-laundering and seems much more well-suited to this end compared to digital systems.[192]

Due to the ledger's tamper-evident nature, it can indeed be difficult to rectify or deleted the corresponding information. What is more, these systems' pseudonymous nature makes it burdensome to track down the identity of the individuals or groups responsible for infringements. This is particularly the case where public and permissionless blockchains use privacy-preserving features, also highlighting important policy tensions

[184] Based on feedback received during the workshop (more information on the workshop can be found in the introduction of this report).
[185] Ibidem.
[186] William Foxley, 'Netherlands May Block Foreign Crypto Firms Under Anti-Money Laudering Laws' (Sept 2019), https://www.coindesk.com/dutch-interpretation-of-eu-anti-money-laundering-rules-may-block-foreign-firms (last accessed on 23 October 2019).
[187] Interview with the Nordic Blockchain Association.
[188]'Guidance 02/2019: Payments on the blockchain' (Finma, August 2019), available at https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20190826-finma-aufsichtsmitteilung-02-2019.pdf?la=en (last accessed on 23 October 2019).
[189] 'Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs) (Finma, Feb 2018), available at https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en (last accessed on 23 October 2019).
[190] Samuel Gibbs, 'Child abuse imagery found within Bitcoin's blockchain' (The Guardian, 20 March 2018), https://www.theguardian.com/technology/2018/mar/20/child-abuse-imagery-bitcoin-blockchain-illegal-content (last accessed on 17 December 2019).
[191] Robby Houben and Alexander Snyers, 'Cryptocurrencies and blockchain', Policy Department for Economic, Scientific and Quality of Life Policies, PE 619.024 (July 2018), available at http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf (last accessed 23 October 2019).
[192] Interview with John Salmon.

between data protection and law enforcement in some domains. Stakeholders have moreover highlighted that whereas compliance at the application level is rather straightforward, difficulties arise where the material in question is found at the network or protocol layers.[193] Given that blockchains are permanent ledgers, these databases can reveal entire chains of transactions over years to law enforcement agencies as soon as these are able to trace identities behind the respective public keys.[194] Indeed, blockchains can serve a perfect audit trail for these purposes.[195] As a reaction, a range of blockchain analysis companies have emerged over the past few years that can assist law enforcement agencies in tracking criminal activity.[196] Of course, this is not the case where cryptocurrencies with strong privacy protections such as ZCash or Monero are used.[197] Here, effective law enforcement can indeed be a bigger challenge, yet again this does not relate to the fact that blockchain technology is used but rather how it is used.

Some blockchain systems such as fetch.ai attempt to integrate machine learning and AI directedly into a decentralised computation stack. This allows for autonomous economic agents that can learn and follow their own ends. Such a system might be useful for identifying and preventing money-laundering but this application is very much in its infancy.[198]

3.2.4. Tension between blockchain reality and legal reality

Blockchains can be used to tracks transfers of ownership of digital or real-world assets. There may, however, be situations where from a legal perspective, ownership changes, yet this is not reflected on-chain. The tension arising where on-chain information may conflict with that in the real-world has been a matter of ongoing discussion.[199] Indeed, many scenarios can be imagined where on-chain data is not up to date or does not correspond to legal reality, for instance where a transfer of property that occurred off-chain is not reflected on-chain or where a nullity is declared by a court of law in relation to a transaction that occurred on-chain, yet there is no automatic updating of the ledger to reflect this changed state of affairs. Legal research has suggested that for that reason, real-world assets cannot be traded on blockchain-based systems, unless design choices are made which necessarily remove all advantages the technology offers over existing solutions.[200]

---

[193] Based on feedback received during the workshop (more information on the workshop can be found in the introduction of this report).

[194] John Bohannon, 'Why criminals can't hide behind Bitcoin' (March 2016), https://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin (last accessed on 17 December 2019).

[195] Op.Cit., EU Blockchain Forum and Observatory, 'Report on Legal and Regulatory Framework for Blockchains and Smart Contracts', p.14.

[196] Thomas Brewster, 'Why investors are betting millions on bitcoin surveillance' (April 2018), https://www.forbes.com/sites/thomasbrewster/2018/04/05/snooping-on-bitcoin-is-big-business/#77fccf002d19 (last accessed 23 October 2019).

[197] EU Blockchain Forum and Observatory, Report on Legal and Regulatory Framework for Blockchains and Smart Contracts, p.14.

[198] Toby Simpson, Humayun Sheikh, Thomas Hain, Troels Rønnow, Jonathan Ward, 'Fetch: Technical Introduction, a decentralized digital world for the future economy' (Feb 2019), available at https://fetch.ai/wp-content/uploads/2019/10/technical-introduction.pdf (last accessed on 17 December 2019).

[199] Reed, Chris and Sathyanarayan, Umamahesh and Ruan, Shuhui and Collins, 'Justine, Beyond Bitcoin – Legal Impurities and Off-Chain Assets' (October 2017), Queen Mary School of Law Legal Studies, Research Paper No. 260/2017. Available at SSRN: https://ssrn.com/abstract=3058945 or http://dx.doi.org/10.2139/ssrn.3058945 (last accessed 23 October 2019).

[200] Edmund-Philipp Schuster, Cloud Crypto Land (November 21, 2018),LSE Legal Studies Working Paper 17/2019. Available at SSRN: https://ssrn.com/abstract=3476678 (last accessed on 17 December 2019).

Some of our interview partners agreed that there can be gap between the information on the blockchain (such as in respect to property of an asset) and legal reality.[201] Others however consider that this issue is more about the public perception than the reality of the industry.[202] Indeed, it has been argued that blockchain does not really create any new challenges compared to other digital environments.[203] Again, this essentially appears to be a question of governance and design. Indeed, the consensus among stakeholders seems to be that this is a technical and governance problem rather than a legal issue.[204] There is nothing that would make blockchains per se unable to reflect changes in legal reality. Rather, what is needed are appropriate design and governance solutions that make it possible to reflect these changes. Whether these changes then defeat the very reasons for using DLT as opposed to other databases remains a question of ongoing discussion.[205] It is worth noting that in the specific domain of real estate, a number of Member States (such as Austria, Croatia, the Czech Republic, Estonia, Germany, Hungary, Slovakia and Slovenia) recognise a constitutive effect of registration in the land registry and the bona fides of such registration is also recognised.[206] If, over time, blockchains or other forms of digital registries are implemented as replacements or alternatives to current registries, Member States should consider the desirability of extending bona fides also to such digital information. This, however, remains a speculative question as no Member State has moved to replace its existing land registry system with a blockchain, despite, for example, an experiment run by Sweden to relocate real estate transactions to blockchain.[207]

Particularly in relation to smart contracts, some have worried about the practical implications of implementing current legal provisions. Where a court were to order that a smart contract was unenforceable (for instance because one or more parties had no capacity to contract) 'the court will be unable to order a rectification of the result, as the outcome cannot subsequently be changed without destroying the logic of smart contracts'.[208] Parties are then often left with the decision of claiming damages from the other party in kind or in money. It has been suggested that in relation to blockchains, damages in kind are difficult to realise, leaving parties with 'damages as the only remedy, invariably subjecting the transferor to the risk of insolvency of the transferee'.[209] However, this is again not an issue that is unique to DLT but may also arise in other technical environments. Others as a matter of fact consider that such issues may be addressed by existing contract law. Indeed, similar issues have been encountered for a long time where information in land and other public registries (from which data also can in principle not be deleted) contrast with legal reality and law has solved this by finding such information void and mark related entries as outdated and/or provide civil law damages where the damage cannot be undone. [210]

[201] Interview with the Swiss Cryptovalley Association.
[202] Interview with Consensys.
[203] Interview with John Salmon.
[204] Based on feedback received during the workshop (more information on the workshop can be found in the introduction of this report).
[205] Edmund-Philipp Schuster, Cloud Crypto Land (November 21, 2018), LSE Legal Studies Working Paper 17/2019. Available at SSRN: https://ssrn.com/abstract=3476678 (last accessed on 17 December 2019).
[206]Christoph U. Schmid ; Christian Hertel, 'Real Procedure Law and Procedure in the European Union', General Report , European University Institute, available at https://www.eui.eu/Documents/DepartmentsCentres/Law/ResearchTeaching/ResearchThemes/EuropeanPrivateLaw/RealPropertyProject/GeneralReport.pdf, page 34. (last accessed on 24 January 2020).
[207]Joon Ian Wong, 'Sweden's blockchain-powered land registry is inching towards reality' (April 2017), https://qz.com/947064/sweden-is-turning-a-blockchain-powered-land-registry-into-a-reality/ (last accessed on 20 January 2020).
[208] Philipp Paech, Law and Autonomous System Series: What is a Smart Contract? (July 2018) https://www.law.ox.ac.uk/business-law-blog/blog/2018/07/law-and-autonomous-systems-series-what-smart-contract (last accessed 23 October 2019).
[209] Ibidem.
[210] Interview with Nina Siedler.

It is worth noting that other jurisdictions have pursued a legislative approach to addressing this concern. Indeed, Liechtenstein addresses possible discrepancies between information on-chain and information in the real world in its so-called 'Blockchain Law'.[211] The Liechtensteinisches *Token- und VT-Dienstleister-Gesetz* (TVTG) foresees the emergence of new middlemen, so-called ‚physical validators' who are in charge of making sure that the purchaser of a token also really purchases the underlying good. These intermediaries are in charge of making sure that the purchase of the token equals the legal transfer of the underlying legal right or obligation.[212]

3.3. Legal issues regarding smart contracts and utility tokens

After having examined some of the general legal issues that have been discussed in relation to blockchain technology we now turn to ponder specific regulatory challenges as they have been debated in relation to specific use cases, namely smart contracts and utility tokens.

3.3.1. Smart contracts

Smart contracts are computer-coded if-then relations that have been used for a long time in many different contexts. With the advent of blockchain technology, they have risen to prominence as smart contracts can also be used on distributed ledgers. Often, a smart contract is but a piece of computer code with no legal significance. Sometimes, however, such code can be used to execute an existing legal contract (such as where a smart contract is used to transfer ownership of an asset from A to B) and some have suggested that the smart contract may be constitutive of a legal contract itself, as can be seen below. This, of course, has raised a number of legal and regulatory debates, including whether legal reform is needed.

The meaning of the term 'smart contract' is controversial in itself. Some literature points out that 'smart contracts' are legal contracts implemented by a particular type of computer code, while others claim that it is a type of code which – when uploaded to a blind consensus platform – precludes operational interference.[213] Nick Szabo, who first introduced the term 'smart contract', considered these to be mechanisms for enforcing legal contracts – computerised transaction protocols executing the contractual terms. Hence, Szabo saw them as a type of code rather than a legal contract.[214] However, these pieces of computer code do not necessarily have to be a legal contract (they can simply be computer code that has no contractual implications) and the terminology can indeed be confusing. Vitalik Buterin, who introduced the terminology of the smart contract into the blockchain space has in fact expressed regret at his choice of terminology, suggesting he should rather have called these tools 'persistent scripts'.[215]

The reality is that smart contracts are computer code that, depending on the precise context of its use, may be considered to constitute a legal contract – or not. Given their nature, they can and have been used in a variety of contexts for a number of decades already, such as vending machines (an example given by Szabo in his early reflections on the topic) or financial transactions. Where used on blockchains, they assume the properties of the underlying infrastructure – such as tamper-resistance or decentralisation – which is the key reason why they have triggered a range of legal discussions.

[211] 'Token- und VT-Dienstleister-Gesetz (TVTG)' (Oct 2019), available at Liechtensteinisches Token- und VT-Dienstleister-Gesetz (TVTG), https://impuls-liechtenstein.li/wp-content/uploads/2019/11/950.6_TVTG_25.10.2019.pdf (last accessed on 17 December 2019).
[212] Ibidem, Article 2.
[213] Tatiana Cutts, 'Smart Contracts and Consumers', LSE Working Papers, April 2019, p.23.
[214] Ibidem, p.23-24.
[215] V. Buterin (October 2018), https://twitter.com/vitalikbuterin/status/1051160932699770882?lang=en (last accessed on 17 December 2019).

Whereas smart contracts are not always contracts, they are also usually not smart in the sense that they are usually neither embedded with what is conventionally referred to as 'Artificial Intelligence' nor do they ever have capacity to independently think and deliberate. Rather, scholarship has divided smart contracts into two distinct categories: those whose enforcement is automated while the conclusion of the contract is done in a traditional way, and those concluded and enforced in a smart way. At the moment, the majority of smart contracts would fall within the first category, but it is expected that the proportions will change with the further development of the smart contract technology.[216]

Smart contracts are considered to have important advantages and disadvantages. They have been said to 'democratise' legal agreements in offering legal certainty even to individuals unable to afford legal counsel.[217] Indeed, it appears that from a legal perspective, the main promise of smart contracts is to automate the execution of agreements and, where the blockchain relied on is configured appropriately, this can be done without the need for a central authority or an external enforcement mechanism. Some, however, also consider that these tools may generate important risks, such as where the related governance framework does not provide for a central authority that could intervene in case there is a problem with the code, as was the case with the DAO hack.[218] Beyond, it has been highlighted that only 'experts are capable of examining the underlying program code (such as that of the smart contract) in order to assess whether the functionality described in the white paper or terms and conditions is accurate in the case of the tokens concerned. The investor must bear the risk of the offeror providing incorrect information'.[219] Below, we turn to some of the key legal questions that have arisen in relation to these technical tools to date.

3.3.1.1. Application of Contract Law

There can be no doubt that existing mechanisms of contract law apply to smart contracts provided that these indeed qualify as legal contracts.[220] As Rühl has argued 'the classic questions of contract law arise also when parties enter into a smart contract. And just like all other contracts, smart contracts demand that the law answers them. The decisive question, therefore, is not whether smart contracts are subject to the law, but rather to which law they are subject'.[221]

Where a smart contract qualifies as a legal contract, national contract law applies. In the EU, no specific 'smart contract' legal regimes have yet been created at supranational or Member State level with the exception of the Italian example highlighted below. The situation is different in the United States where a number of states have legislated in this respect.[222] In the United States, although the majority of states have yet to consider and/or propose legislation, some states have either proposed or enacted legislation

[216] Mateja Durovic, Andre Janssen, 'The Formation of Blockchain-based Smart Contracts in the Light of Contract Law', European Review of Private Law, Volume 26, 2018, p.757-761.
[217] Also see Oscar Borgogno, 'Smart Contracts as the (new) Power of the Powerless? The Stakes for Consumers' (2018), Vol. 26, European Review of Private Law, Issue 6, 885-902.
[218] 'Blockchain-Technologie' (June 2017), https://www.bafin.de/DE/Aufsicht/FinTech/Blockchain/blockchain_artikel.html (last accessed 23 October 2019).
[219] 'Initial Coin offerings: High risks for consumers' (November 2017), https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2017/fa_bj_1711_ICO_en.html (last accessed on 23 October 2019).
[220] Chamber of Digital Commerce, 'Smart contracts: Is the Law Ready?' (Sept 2018), available at https://digitalchamber.org/smart-contracts-whitepaper/ (last accessed 23 October 2019), p.17-18.
[221] Giesela Rühl, 'The Law applicable to smart contracts, or much ado about nothing?' (Jan 2019), available at https://www.law.ox.ac.uk/business-law-blog/blog/2019/01/law-applicable-smart-contracts-or-much-ado-about-nothing (last accessed on 23 October 2019).
[222] Arizona - AZ HB2417, Tennessee - TN SB1662, Vermont - VT S0269, Wyoming SF 0125.

applicable to smart contracts or contracts in electronic format.[223] Some examples of this can be found in the table below.

Table 1 – Examples of US state legislation on smart contracts

Arizona	AZ HB2417 | 2017 Passed on 29 March 2017	Allows the use of smart contracts in commerce and prevents the document from being denied legal effect solely because it includes a smart contract term. Also recognises signatures and records secured using blockchain technology as valid recognised electronic signatures and records under state law.
Tennessee	TN SB166 2 | 2017-18 Passed on 26 March 2018	Recognises legal authority to use DLT and smart contracts when conducting transactions. Protects ownership rights of certain information secured by distributed ledger technology.
Vermont	VT S0269 | 2017-18 Passed on 30 May 2018	Creates a special class of Limited Liability Company (LLC) called a Blockchain-Based Limited Liability Company (BBLLC). These BBLLCs are those that are allowed to use blockchain technology for all or some aspects of its corporate governance, including using smart contract executed voting procedures for various internal decision-making scenarios.
Wyoming	SF 0125 | 2019 In effect from 1 July 2019	"An act relating to property; classifying digital assets within existing laws; specifying that digital assets are property within the Uniform Commercial Code; authorising security interests in digital assets; establishing an opt-in framework for banks to provide custodial services for digital asset property as custodians; specifying standards and procedures for custodial services under this act; clarifying the jurisdiction of Wyoming courts relating to digital assets; authorising a supervision fee; making an appropriation; authorising positions; specifying applicability; authorising the promulgation of rules; and providing for an effective date."

However, it has been argued that smart contracts would already have been enforceable under general federal contract law principles in the United States.[224] The Electronic Signatures in Global and National Commerce Act (ESIGN Act) as well as the Uniform Electronic Transactions Act (UETA) have been said to provide sufficient legal basis for smart contracts that are embedded with the terms of a legal contract so as to not have required any additional bespoke legislation.[225]

[223] Legal research questionnaire for the US.
[224] 'Blockchain and Cryptocurrency Regulation 2020, 13 legal issues surrounding the use of smart contracts', https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/13-legal-issues-surrounding-the-use-of-smart-contracts#chaptercontent5 (last accessed on 17 December 2019).
[225] Chamber of Digital Commerce, '"Smart Contracts" Legal Primer: Why Smart Contracts Are Valid Under Existing Law and Do Not Require Additional Authorization to Be Enforceable' (Jan 2018), available at https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-Legal-Primer-02.01.2018.pdf (last accessed on 17 December 2019).

Seen from this perspective, there is a danger that additional state legislation has added complexity and fragmentation that might ultimately be detrimental to innovation. These state legislative efforts also have enshrined bad definitions of the technology in law. The Arizona Act for instance speaks of an 'immutable ledger' that 'provides an uncensored truth'. This is obviously misguided as blockchains are neither strictly immutable nor do they provide any guarantee that registered information is truthful.[226] This not only generates interpretational difficulties but fails to make the legislation technology-neutral. Indeed, the varying definitions of blockchain 'may create unintended roadblocks to innovation by creating unnecessary ambiguities and litigation'.[227]

Although most jurisdictions do not recognise a bespoke legal category of the smart contract, the latter will often be caught by established definitions of contract law where they are also legal contracts. This relates to the fact that most jurisdictions recognise the principle of freedom of contract, which oftentimes includes that there is also freedom over the form of the contract that is chosen.[228] According to that principle, contracts can also be concluded electronically.[229]

As a consequence, a smart contract is a legal contract where it meets the legal requirements for contract formation (which somewhat diverge between jurisdictions, particular between common law and civil law countries) and this irrespective of whether it takes the form of a written, oral or blockchain-based smart contract written in computer code.[230] This is important to stress, also because the use of smart contracts does not make commonplace issues of contract law disappear. Indeed, as noted by the EU's Blockchain Observatory and Forum, 'the use of smart contracts does not resolve or eliminate the problem of breaches of contract, contractual liability and enforcement'.[231]

As fully digital ledgers, blockchains are by definition electronic documents under eIDAS (as per Article 35 eIDAS, electronic documents are any documents with electronic content). That means that blockchains, or more properly the data, including smart contracts, contained in them, cannot be denied legal force, at least not solely because of their electronic nature. This is also reflected in Member State law. In Italy, paragraph 3 of Article 8-ter, Law 11 February 2019 states that the storage of an IT document using distributed ledger technologies produces the legal effects of the electronic time stamp pursuant to Article 41 of Regulation (EU) No. 910/2014.

In the United States, valid signatures are broadly defined, which means an electronic signature should be deemed sufficient to establish the identity of parties relying on a cryptographic signature for a smart contract.[232] In the US Uniform Electronic

[226] Also see: Angela Walch, 'The Path of the Blockchain Lexicon (and the Law)' (March 24, 2017), 36 Review of Banking & Financial Law 713 (2017). Available at SSRN: https://ssrn.com/abstract=2940335 (last accessed on 18 December 2019).
[227] Cardozo Blockchain Project, 'Smart Contract and Legal enforceability', Research Report n°2 (October 16, 2018), available at https://cardozo.yu.edu/sites/default/files/Smart%20Contracts%20Report%20%232_0.pdf, p.26. (last accessed on 17 December 2019).
[228] Legal research questionnaire for Germany.
[229] For Singapore, see *Chwee Kin Keong & Ors v Digilandmall.com Pte Ltd* [2004] 2 SLR(R) 594.
[230] For an example of rules regarding contract formation, see Article 1325 of the Italian Civil Code.
[231] Report of the EU Blockchain Observatory and Forum, 'Legal and Regulatory Framework of Blockchains and Smart Contracts' (2019), p.21, available at https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf?width=1024&height=800&iframe=true (last accessed on 23 October 2019).
[232] Lamle v. Mattel, Inc., 394 F.3d 1355, 1361 (Fed. Cir. 2005) ("we conclude that under California law the . . . email satisfies the Statute of Frauds."); Levin v. Knight, 780 F.2d 786, 787 (9th Cir. 1986) 34 Willmott v. Giarraputo, 157 N.E.2d 282, 282 (N.Y. 1959); Brown v. Cara, 420 F.3d 148, 150 (2d Cir. 2005); Huntington Towers, Ltd. v. Franklin Nat'l Bank, 559 F.2d 863, 864 (2d Cir. 1977); Canister Co. v. Wood & Selick, Inc., 73 F.2d 312, 315 (3d Cir. 1934); Conner v. Lavaca Hosp. Dist., 267 F.3d 426, 430 (5th Cir. 2001).

Transactions Act (the 'ETA'), an 'electronic signature' is defined as "an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record."[233] A cryptographic key is likely to constitute a record of a 'process' (within the meaning of the ETA), which is associated with a record, or it has a symbol constituting a signature and thus recorded on the DLT. Therefore, this key would be essential to the form of the agreement, and more so could be used as a condition for the validity of the smart contract itself.

Article 25 of the eIDAS Regulation furthermore states that an electronic signature shall not be denied legal effect as evidence in legal proceedings solely on the grounds that it is in electronic form, and that a qualified electronic signature shall have the equivalent legal effect of a handwritten signature. [234] A review of domestic provisions on contract law moreover underlines that smart contracts will usually be caught by national laws on electronic contracts. For instance, in German law, paragraph 312j of the BGB creates a special regime for electronic contracts that are concluded with consumers, in relation to information that needs to be made available to the consumers on the website prior to them ordering any goods.[235]

French law also explicitly recognises electronic contracts.[236] In Spain, Law 34/2002 for the Information Society and Electronic Commerce Services regulates electronic contracts.[237] Article 23 of this legislation specifies that it is not necessary a prior agreement between the parties regarding the use of electronic means. It further provides that when the law requires that the contract, or any information related to it, must be in writing, this requirement is fulfilled if the contract or information is contained on electronic support. Where specific legal regimes exist in relation to electronic contracts, smart contracts will usually fall within their scope of application. Similarly, other Member States also have legislation on electronic contracts that would apply to smart contracts.[238]

Important questions also arise regarding contract validity. As has been seen above, one of the main legal doubts arising in reference to smart contracts is whether they are, in fact, contracts from a legal point of view. This may lead to doubts concerning the possibility to enforce of smart contracts and whether they are entered into with the intention of being judicially enforceable at all.[239]

Regarding the validity of smart contracts, their digital form is likely not problematic as most jurisdictions allow contracts to be expressed in any form chosen by the parties.[240] The parties to the contract (humans) submit the cryptographic private keys to blockchain-based smart contracts. Depending on the specificities of the respective smart contract, two scenarios can be imagined. First, a one-sided scenario whereby the smart contract could be designed so that anyone could enter into a contractual relationship by executing a function of the smart contract. Second, a two-sided scenario whereby

[233] Article 40, Uniform Electronic Transactions Act, https://www.ncleg.net/EnactedLegislation/Statutes/PDF/ByArticle/Chapter_66/Article_40.pdf (last accessed on 23 October 2019).
[234] Regulation (EU) 910/2014 on the electronic identification and trust services for electronic transactions in the internal market, OJ, L 257, Vol. 57, 24 August 2014.
[235] Legal research questionnaire for Germany.
[236] Articles 1125 – 1127-4 and 1174-1177 du Code Civil modifiés par Article 2 de l´Ordonnance n°2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations.
[237] Articles 23- 29 of the Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Available at: https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758.
[238] For Italy, see Legislative Decree No. 70/2003.
[239] Kevin Werbach, Nicolas Cornell, 'Contracts ex Machina', Duke law journal, available at https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3913&context=dlj, (last accessed on 23 October 2019), p.341-343.
[240] In English law, email communication can give rise to a legally binding contract.

anyone is invited to make an offer (by executing a function of the smart contract) and the party deploying the smart contract as well as the counterparty have to accept the offer before a legal contract comes into place.[241]

Article 9 of the E-Commerce Directive further requires that Member States allow contracts to be concluded by electronic means (in B2B and B2C relations).[242] To be enforceable, contracts in electronic form must nonetheless satisfy the relevant validity requirements in domestic contract law.[243] In common law jurisdictions a valid contract requires: (i) offer and acceptance, (ii) consideration, (iii) an intention to create legal relations[244], and that (iv) the agreement is either complete (it does not lack essential terms) or certain (the terms are not ambiguous or vague). In civil law jurisdictions, requirements differ. Under French civil law three key elements ought to be present, namely (i) consent that is to say a mutual agreement through offer and acceptance, (ii) legal capacity to enter a contract, (iii)a lawful and certain content.[245] The French Civil Code also recognises that contracts can take an electronic form.[246]

It accordingly appears that no specific blockchain-related issues emerge in relation to contract formation and validity. The law seems to be operating in a technologically-neutral manner and does not, per se, disadvantage DLT compared to other digital solutions. Whereas legal requirements certainly exist, these fulfil important public policy objectives and our research has not revealed that this would have detrimental effects for innovation in the blockchain realm.

It might be argued that this conclusion is problematic at infrastructure level, particularly for public and permissionless blockchains in that the technology itself cannot differentiate between users. Yet, other forms of databases are unable to themselves recognise whether a user or entry is (or an entry in the database relates to) a natural or legal person, a consumer or trader, or a person from jurisdiction A or B. Similarly, infrastructure itself (such as the Internet) is also not conventionally expected to fulfil that role. Rather, what can be observed from these other scenarios is that processes and tools have developed around the infrastructure itself that enable the identification of individuals for purposes of defining, for instance, matters of jurisdiction, or whether consumer law applies or not. As additional layers (such as applications) are being developed on top of blockchain there are no indications that they would be able to fulfil that role.

One element deserving particular attention is that of smart contracts' cross-border dimensions as it is expected that they will underpin data ecosystems that span entire continents or even operate globally. For instance, a company from Member state A could equip a car with an automated tool using smart contracts that would regulate payments at toll stations or gas stations. However, the owner or renter of the car might want to also rely on this tool when paying fees or gas in Member State B. For this to happen,

[241] Op. Cit., Mateja Durovic, Andre Janssen, p.762; Kevin Werbach, Nicolas Cornell, 'Contracts ex Machina', Duke law journal, available at https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3913&context=dlj (last accessed on 23 October 2019), p.330.
[242] Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market, OJ, L 178, Vol. 43, 17 July 2000.
[243] Mateja Durovic and André Janssen, 'The Formation of Blockchain-Based Smart Contracts in the Light of Contract Law' (2018), European Review of Private Law available at http://static.ie.edu.s3.amazonaws.com/Tertulia/Papers%202018/Papers/The%20Formation%20of%20Blockchain-based%20Smart%20Contracts%20in%20the.pdf (last accessed on 23 October 2019), p.753-771.
[244] Which is assessed objectively as per RTS Flexible Systems Ltd v Molkerei Alois Muller Gmbh & Company KG (UK Production) [2010] UKSC 14, at paragraph 45.
[245] See Ordonnance n°2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations and Article 1101 and 1128 of the French Civil Code.
[246] Article 1102 of the French civil code.

technical but also legal interoperability between systems are paramount. Or one might imagine that a company from Member State C requires file storage and buys redundant capacity from a server located in Member State C through a matchmaking platform located in a jurisdiction outside of the EU.

The exchange of file storage (through an API key) and the remuneration (a token) occur automatically based on a smart contract that operates on a blockchain. The buyer and seller do not know one another, their identity is not disclosed by the matchmaking platform. If something goes wrong (imagine the storage capacity not being available while the token has been transferred) a dispute arises, which raises the question of the validity of the platform's terms and conditions that exclude liability for the performance of a contract that is concluded through the matchmaking platform. Particularly in the absence of the written contract this would raise the question of whether a valid legal contract been has concluded between the buyer and seller of storage capacity and whether the contract would be valid in all jurisdictions that are involved.

The above examples thus highlight that the enforceability of smart contracts across the borders of various Member States is indeed an important topic from a Digital Single Market perspective, as smart contracts are expected to be used (among other things) in context of past-paced multi-jurisdictional contexts.

It has been suggested in relation to some countries that where the smart contract is the means of executing a natural language contract, courts would consider the overall context: the smart contract, the related semantic contract, and any additional coding or documentation to determine whether there is a legally binding contract between the parties and, if so, what its terms are.[247] In this context, courts would likely find that the semantic contract prevails (unless it can be concluded that the parties' intention is proof of the contrary) and the legal issues raised in this context would be no different from disputes regarding the enforceability of any other contract. [248]

The smart contract can be the legal contract itself (as opposed to merely a means of enforcing it).[249] In such a case, the computer code itself would include the legal agreement in its entirety.[250] There are two situations when this would be the case: when the code indeed contains the entire agreement between the parties or where it prevails over any other clauses, formulated in natural language.[251] The code could also form only an integral part of the legally binding contract and not the entirety of the contract. In such a case, the smart contract may still to an extent be supported by the natural

[247] 'SMART CONTRACTS: Is the Law Ready', Digital Chamber of Commerce, SMART CONTRACTS ALLIANCE, September 2018, available at https://lowellmilkeninstitute.law.ucla.edu/wp-content/uploads/2018/08/Smart-Contracts-Whitepaper.pdf (last accessed on 19 December 2019); confirmed by the legal research questionnaires which can be found in Annex III.
[248] SMART CONTRACTS: Is the Law Ready, Digital Chamber of Commerce, SMART CONTRACTS ALLIANCE, September 2018, available at https://lowellmilkeninstitute.law.ucla.edu/wp-content/uploads/2018/08/Smart-Contracts-Whitepaper.pdf (last accessed on 19 December 2019).
[249] Report of the EU Blockchain Observatory and Forum, 'Legal and Regulatory Framework of Blockchains and Smart Contracts' (2019), page 23.
[250] SMART CONTRACTS: Is the Law Ready, Digital Chamber of Commerce, SMART CONTRACTS ALLIANCE, September 2018, available at https://lowellmilkeninstitute.law.ucla.edu/wp-content/uploads/2018/08/Smart-Contracts-Whitepaper.pdf (last accessed on 19 December 2019). , p.25; Somto Kizor – Akaraiwe: Smart Contracts, Copyrights and Artificial Intelligence, 27/04/2019, available at https://www.researchgate.net/publication/335273097_Smart_Contracts_Copyrights_and_Artificial_Intelligence/link/5d5c07e792851c37636c1557/download (last accessed on 19 December 2019), p.4-5.
[251] SMART CONTRACTS: Is the Law Ready, Digital Chamber of Commerce, SMART CONTRACTS ALLIANCE, September 2018, available at https://lowellmilkeninstitute.law.ucla.edu/wp-content/uploads/2018/08/Smart-Contracts-Whitepaper.pdf, last accessed 19/12/2019, p.25; Somto Kizor – Akaraiwe: Smart Contracts, Copyrights and Artificial Intelligence, 27/04/2019, available at https://www.researchgate.net/publication/335273097_Smart_Contracts_Copyrights_and_Artificial_Intelligence/link/5d5c07e792851c37636c1557/download, last accessed 19/12/2019, p.4-5.

language version: for instance in relation to non-operational clauses. However, it needs to be noted that the code would have the legal effect. This means the code would constitute an integral part of the agreement and not merely a translation of its terms. In operating certain clauses, the code would constitute the legally binding contract between the parties.[252] It is, however, worth noting that this is rare and particularly so in the EU. Indeed, where there is a consumer contract, the E-Commerce Directive obliges traders to provide information to consumers in a manner that is understandable to them.[253] Thus, smart contracts that are also legal contracts can only be used where the necessary safeguards are implemented in B2C settings – just as is the case with any other electronic contract.

National legislation impacts on what form of smart contract can be used in what context. For instance, where national law requires a written contract, a smart contract consisting only of the computer code would not be enforceable whereas a combination of semantic and smart contract likely would be. Indeed, our research has revealed that a number of jurisdictions have such requirements. In France, an electronic contract in principle satisfies the requirement for a contract to be in writing, except in some circumstances such as acts under private signature relating to family law and inheritance[254] or acts under private signature relating to personal or real security, of a civil or commercial nature, except if they are passed by a person for the needs of his profession.

Under German law, employment contract, a fixed-term rent contracts and public law contracts need to be in writing[255] although, in general, the electronic conclusion of a contract (as long as a qualified electronic signature is used)[256] fulfils the written form requirement unless notarisation is required.[257] Where that is the case, a smart contract originating from another Member State may not be enforceable in Germany. In cases where there is a divergence between jurisdictions as to related requirements, or indeed any other requirement such as those deriving from contrasting national interpretations of order public, there is a risk that – just as is the case for semantic contracts – smart contracts cannot be recognised in all Member States.

It is, however, worth recalling that in principle parties have a choice of the jurisdiction and it has been argued that it will usually be possible to assign a smart contract to a particular legal system based on Rome I Regulation. The Rome I regulation determines the governing law of a contract in the absence of express agreement between the parties. By default, if the parties to a contract agree that a governing law (e.g. the law of England and Wales) should apply to a contract then that law is the one which will usually be applied.[258] If, however, the parties have not agreed on an applicable law for their legal relationship then Rome I contains a series of rules to decide which law applies. Typically, this will be one party's country of residence although contracts concerning rights in land (including leases) will typically be governed by the law of the country in which the property is located. By way of example, an agreement for the sale of goods is governed by the law of the country where the seller is habitually resident. Although

[252] SMART CONTRACTS: Is the Law Ready, Digital Chamber of Commerce, SMART CONTRACTS ALLIANCE, September 2018, available at https://lowellmilkeninstitute.law.ucla.edu/wp-content/uploads/2018/08/Smart-Contracts-Whitepaper.pdf, last accessed 19/12/2019, p.26; Smart Contracts, Copyrights and Artificial Intelligence, 27/04/2019, available at https://www.researchgate.net/publication/335273097_Smart_Contracts_Copyrights_and_Artificial_Intelligence/link/5d5c07e792851c37636c1557/download, last accessed 19/12/2019, p.4-5.
[253] Article 10 of Directive 2000/31/EC.
[254] Except agreements signed under private signature countersigned by lawyers in the presence of the parties and filed at the rank of the minutes of a notary in the manner provided for in articles 229-1 to 229-4 or 298.
[255] Paragraph 126 BGB.
[256] Paragraph 126a BGB.
[257] Paragraph 126(3) BGB.
[258] Article 3(1) of the Rome I Regulation.

the Rome I regulation provides a fall-back to allow EU state courts to work out which law should apply to the agreement, it is highly recommended that an express jurisdiction clause be included in the agreement for certainty, particularly in B2B contexts where the B2C default rules under EU law do not apply in order to increase legal certainty for the parties to the contract. Indeed, this regime does not rely on the place of formation or the place of performance to determine the applicable law, but resorts to connecting factors, namely party choice and habitual residence, which work reasonably well in a globalised and digitalised society.[259]

It is worth noting that Article 1(2)(d) of the Rome I Regulation excludes from its scope 'obligations arising under bills of exchange, cheques and promissory notes and other negotiable instruments to the extent that the obligations under such other negotiable instruments arise out of their negotiable character'. This is an interesting provision in relation to cryptoassets in general as some of them could qualify as 'negotiable instruments'. In relation to those cryptoassets which are the focus of the present report, namely utility tokens, their lack of negotiability is, however, often stressed. Indeed, as will be seen below, utility tokens are primarily designed for on-platform use and where they are tradable on secondary markets this oftentimes does not result from the initiative of the issuer. As such, it cannot be assumed that utility tokens in general qualify as negotiable instruments.

Under English law, a contract is only then concluded when terms and conditions of a one party to the contract are adopted by the other party (also in a conclusive way by an action/performance) – so reference to international private law is not needed.[260] Germany also recognises that parties have a choice as to which law is to govern their contract. If parties fail to make a choice in this respect and B2B there are general terms and conditions that choose different jurisdictions, international private law is applied to determine applicable law.[261] In B2B contexts, where parties have not concluded a choice of jurisdiction agreement, the legal assessment of the dispute shall take place in accordance with the provisions of the UN Sales Convention (CISG).[262]

It follows that there can be scenarios where the cross-border circulation of smart contract is hindered, such as where Member State A (in which the contract is concluded) has no specific requirements regarding the form of the contract, but Member State B requires that it be in writing for it to be valid. However, existing mechanisms such as the Rome I regime and additional public international law principles appear well-suited to deal with such tensions.

3.3.1.2. The need for written form of the contract

It has been seen above that in some circumstances, a blockchain-based smart contract may qualify as a legal contract (namely where it meets all requirements for contract formation under domestic law) without, however, necessarily having a written contract

[259] Giesela Ruhl, 'The law applicable to smart contracts or much ado about nothing' (Jan 2019), available at: https://www.law.ox.ac.uk/business-law-blog/blog/2019/01/law-applicable-smart-contracts-or-much-ado-about-nothing. (last accessed on 18 December 2019).

[260] Holger Ette, Das Kollisionsrecht grenzüberschreitender Überweisungen: Kollisionsrecht und Kollisionsrechtspraxis in Deutschland, England und den USA (The collision law of cross-border transfers: conflict of laws and collision law practice in Germany, England and the USA) , 2013. *See also Berrocal v Warner Chappell Music Ltd (unreported), 3 October 2017 (IPEC).*

[261] Holger Ette, Das Kollisionsrecht grenzüberschreitender Überweisungen: Kollisionsrecht und Kollisionsrechtspraxis in Deutschland, England und den USA (The collision law of cross-border transfers: conflict of laws and collision law practice in Germany, England and the USA), 2013.

[262] Judgment of the Regional Court of Fulda (LG Fulda) 2 O 681/14 of 29/09/2015 available at https://openjur.de/u/2189179.html (last accessed on 198December 2019). See also Federal Court of Germany, Judgment of 31/10/2001, VIII ZR 60/01, available at https://openjur.de/u/62229.html) (last accessed on 18 December 2019).

existing analogously to the computer code. The question thus arises whether this computer code could in itself be considered to constitute a contract or whether the contract needs to be written in prose for it to have legal effects. It has been stressed in the legal literature that it is important to distinguish between whether a contract has been concluded in writing and implemented through blockchain, which is said to raise fewer issues, compared to situations where there is no such parallel requirement.[263] However, it is also important to note that in some circumstances the existence of a parallel written contract may not just make things easier but this may also be a legal requirement.

Our research has shown that most jurisdictions allow parties to, in principle, choose the form of the contract. For example, under Italian law, freedom of form is the principle. Article 1325 of the Italian Civil Code stipulates that the written form is not necessary in order for a contract to exist, unless a specific form is requested (i.e. written form). In Spain, a contract is binding, regardless of form, as long as it meets all essential requirements regarding its validity.[264] However, in almost all jurisdictions exceptions from the general principle of freedom of form can be identified. For instance, Italian law requires that certain contracts take a written form, either for the purposes of giving evidence (*ad probationem*) (e.g., for a settlement agreement) or as a validity requirement (*ad substantiam*) (e.g. contract related to real estate).[265] In Germany, paragraph 126 of the BGB requires this for employment contracts, fixed-term rent contracts and public law contracts. [266]

Some Member States however explicitly provide that the requirement of having the contract be in writing can also be fulfilled electronically. In Spain, Article 23.3 of Law 34/2002 establishes that when the law requires that the contract, or any information related to it, must be in writing, this requirement is fulfilled if the contract or information is contained on electronic support. It should be noted, however, that where a consumer is part of the contract, there is a requirement for legibility. Indeed, Article 8.1 of Directive 2011/83/UE provides that for distance contracts, traders shall provide information "in plain and intelligible language. In so far as that information is provided on a durable medium, it shall be legible". This article has been transposed into the Spanish legislation.[267] Articles 10(1)(a) and (c) of the E-Commerce Directive further provide that in consumer contracts, service providers ought to give clear, comprehensive and unambiguous information (prior to the placing of the order by the service recipient) regarding at least (i) the different technical steps needed to conclude the contract, and (ii)the technical means for identifying and correcting input errors prior to the placing of the order. The requirement for legibility also applies to any contract term which has not been individually negotiated with the consumer.[268] Computer code in the form of 1s and 0s would hence likely not meet related requirements.

Furthermore, electronic contracts between professionals and consumers (B2C) are subject to certain specificities such as that a consumer who has entered into an agreement that has been drafted by a commercial entity has the right to obtain the terms and conditions of a contract on paper at any time. Failure to comply may nullify

[263] See, e.g. Elise Melchior, 'Réflexions juridiques autour de la blockchain: analyse sous l'angle du droit des contrats' (2019), 72 Revue du droit des technologies de l'information 45. (Arguing that the validity of the smart contract in the sense of contract law is not necessarily an issue where there is a written contract together with the paper contract).
[264] See Article 1278 of the Civil Code and Article 51 of the Commercial Code.
[265] Legal research questionnaire for Italy.
[266] Legal research questionnaire for Germany.
[267] Article 98.1 of Consolidated text of the General Consumer and User Protection Act and other supplementary laws passed by Legislative Royal Decree 1/2007 of 16 November 2007.
[268] Article 80.1. b) of Consolidated text of the General Consumer and User Protection Act and other supplementary laws passed by Legislative Royal Decree 1/2007 of 16 November 2007.

the contract that would otherwise have formed.[269] This may prove challenging in some contexts where the corresponding governance mechanisms are lacking (such as public and permissionless blockchains) but likewise, these problems can also emerge where other databases are used.

In France, where a writing is required for the validity of a contract, it may be established and kept in electronic form.[270] Where a written mention is required of the person who binds herself, the latter may affix it in electronic form if the conditions of such affixing are such as to guarantee that it can only be carried out by himself. A number of exceptions however exist such as for acts under private signature relating to family law and inheritance, except agreements signed under private signature countersigned by lawyers in the presence of the parties and filed at the rank of the minutes of a notary.[271] A further exception is that of acts under private signature relating to personal or real security, of a civil or commercial nature, except if they are passed by a person for the needs of his profession. Furthermore, where paper writing is subject to special conditions of readability or presentation, the electronic writing must meet equivalent requirements.[272]

Also jurisdictions outside of the EU have specific laws designed to facilitate the use of electronic contracts. Various domestic regimes on electronic contracts indeed foresee that a contract can be validly concluded without the need for it to be written in prose. For instance, in Singapore, the Electronic Transmissions Act (the 'ETA') implements the United Nations Convention on the Use of Electronic Communications in International Contracts that was adopted by the General Assembly of the United Nations on 23rd November 2005. The ETA provides legal recognition of electronic records and electronic signatures if the electronic signature can reliably identify the person and indicate that person's intentions in respect of the information contained in the electronic record.[273] The legislation also expressly states that offer and acceptance can be expressed by electronic communications, and contracts shall not be denied validity or enforceability solely on the grounds that electronic communications were used in its formation.[274] In other words, electronic contracts – including smart contracts – are not invalid or unenforceable simply because they are electronic.[275]

At EU level, the 2018 Renewable Energy Directive does also provide a definition of a tool that could be understood to be a smart contract. Indeed, its Article 2(18) reads as follows: 'peer-to-peer trading' of renewable energy means the sale of renewable energy between market participants by means of a contract with pre-determined conditions governing the automated execution and settlement of the transaction, either directly between market participants or indirectly through a certified third-party market participant, such as an aggregator. The right to conduct peer-to-peer trading shall be without prejudice to the rights and obligations of the parties involved as final customers, producers, suppliers or aggregators'.

[269] Also see Articles 7, 8 and 9 of Law 22/2007, Of July 11, On Distance Marketing Of Financial Services To Consumers.
[270] Article 1174, French Civil Code.
[271] Article 1175, French Civil Code.
[272] Article 1176, French Civil Code.
[273] See Sections 6 and 8 of the ETA, respectively.
[274] Sections 11(1) and (2) ETA.
[275] In Chwee Kin Keong & Ors v Digilandmall.com Pte Ltd [2004] 2 SLR(R) 594, the Court observed that the "ETA is essentially permissive. It does not purport to regulate e-commerce but attempts to facilitate the usage of e-commerce by equating the position of electronic records with that of written records, thus elevating the status of electronic signatures to that of legal signatures." Also see *Chwee Kin Keong & Ors v Digilandmall.com Pte Ltd [2004] 2 SLR(R) 594 ("Digilandmall")* available at http://www.cisg-online.ch/content/api/cisg/urteile/1641.pdf (last accessed on 23 October 2019).

Beyond, it is worth noting that Italy is the first Member State to have explicitly addressed this in relation to smart contracts. Here, smart contracts have been defined in law as the conversion of an agreement between two or more parties into a computer program which is capable of verifying that certain conditions/events are triggered and, thus, automatically execute certain actions. Once the relevant ledger entry has been validated, it automatically gives effect to the relevant terms agreed between two or more parties. Basically, on the occurrence of predefined events the smart contract is enforced.[276] Thereby, smart contracts on distributed ledger technologies are considered entered into in writing if the Agid (Agency for Digital Italy)'s guidelines are complied with. It is worth noting, however, that to date the Agid has yet to issue any such guidelines. Moreover, to ensure that smart contracts are concluded in writing, an electronic signature system that is able to identify the parties must be in place. The system must be an advanced electronic signature or a qualified one.[277] As a consequence, it is possible that the requirement that smart contracts comply with such guidelines, coupled with the fact that no guidelines have yet been issued will inhibit the deployment of smart contracts in Italy. Moreover, it is worth wondering whether the definition of a smart contract as 'the conversion' of an agreement between two or more parties into a computer program excludes those smart contracts that do not have a paper contract counterpart (and for which none is required by law). If so, there is a risk that these rules may impede the deployment of smart contracts from other Member States in Italy.

The National Council of Notaries (the board representing notaries in Italy), considers that smart contracts are software deployed on blockchains.[278] Law no. 12/2019 indeed foresees that only smart contracts which operate with DLTs are a 'smart contract' (although, as noted above, smart contracts can also rely on other technologies for deployment). This restrictive definition may prove problematic in the long term as it excludes smart contracts relying on other technologies. As such, one may wonder whether this national legislation lives up to the ideal of technological neutrality. Furthermore, one may wonder whether smart contracts can be qualified as legal contracts under Italian civil law. While Article 8-ter paragraph 2 of Law no. 12/2019 defines smart contracts as 'computer programs', the effects described in that article can lead to an interpretation of a smart contract either as an execution tool of a pre-existing contract (performance) or a contract within the strictest, civil law meaning (binding nature for the parties).

It is worth noting that the Italian legislation also addresses compatibility with eIDAS as it provides that the uploading of a file onto DLT has "the legal effect of the electronic time stamp pursuant to article 41 of Regulation (EU) no. 910/2014", provided that the DLTs meet the technical standards which will be released by the Agid.[279]

3.3.1.3. Smart contracts and Consumer Law

Smart contracts are also caught by existing norms of EU law. In cases where a blockchain-based smart contract also qualifies as a legal contract, existing instruments of consumer law such as the E-Commerce Directive[280] and the Consumer Rights

[276] Article 8-ter, Law 11 February 2019, n. 12 (Simplification Law).
[277] On these requirements, also see Digital Administration Code (CAD) (Legislative Decree No. 82/2005, as amended by Legislative Decree 179/2016) and by the EU Regulation No. 910/2014 (eIDAS Regulation).
[278] Consiglio Nazionale del Notariato, 'Smart Contract e tecnologie basate su registri distribuiti – Prime note' (Marzo 2019), L.12/2019, available at https://www.notariato.it/sites/default/files/S-1-2019-DI.pdf (last accessed on 18 December 2019).
[279] Art. 8-ter paragraph 3 and 4 of Law n. 12/2012.
[280] 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, available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031 (last accessed on 15 November 2019).

Directive[281] prima facie also apply in B2C relations. It is, however, worth enquiring if smart contracts really fall within the scope of the Consumer Rights Directive. Indeed, its Article 3(2)(l) excludes its application to contracts 'concluded by means of automatic vending machines or automated commercial premises'. The analogies between smart contracts and vending machine sales have been drawn to illustrate the automated nature of both sets of transactions.[282] Furthermore, existing guidance from the Commission underlines that this exemption ought to be interpreted in a broad manner, such as to also catch automated petrol stations without the physical presence of the trader's representative for the conclusion of the contract.[283] Whereas this is a matter ultimately to be clarified by the Court of Justice of the European Union, Article 3(2)(l) of the Consumer Rights Directive appears to give rise to a presumption that a smart contract which is itself the legal contract (a scenario that is so far rare, as underlined above) may not be caught by this legal instrument (whereas legal contracts that merely use a smart contract to execute an element of the contract will likely be caught).

If the issuer is a business undertaking and the buyer a consumer, they will moreover also be subject to the Unfair Commercial Practices Directive.[284] This is important as it has been stressed in the legal literature that although computer code has the capacity to act as a form of law, state-sanctioned law needs to apply where the rights and interests of others are threatened.[285] This may be the case in relation to consumer contracts where state-sanctioned law has traditionally served to protect the interests of the weaker party.

It will be seen below that consumer and investor protection has also been identified as an important concern in relation to blockchain-based utility tokens. This thus appears to be an issue that ranks high on the list of regulatory concerns related to DLT. In particular smart contracts that trigger automated transactions and are characterised by high complexity can be problematic as non-experts cannot grasp what the smart contract actually transposes at a technical level (and to what degree this may correspond to the parallel written contract). As a result, the German government's blockchain strategy ponders that it may be desirable to create additional informational obligations that apply in such contexts and provide users with information about the content of the smart contract (its code) in a manner that is easy to understand.[286] It furthermore sees this as an important building block towards a higher acceptance and proliferation of smart contracts.[287] It is also worth noting, however, that the German

[281] 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, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0083 (last accessed on 15 November 2019).
[282] Nick Szabo, Smart Contracts: Building Blocks for Digital Markets (1996), http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature (last accessed on 24 January 2020). .
[283] 'DG JUSTICE GUIDANCE DOCUMENT on the Directive 2011/83/EU on consumer rights', available at https://ec.europa.eu/info/sites/info/files/crd_guidance_en_0_updated_0.pdf, page 10. (last accessed on 24 January 2020).
[284] 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, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32005L0029, (last accessed on 15 November 2019).
[285] Karen Yeung, 'Regulations by Blockchain: the Emerging Battle for Supremacy between the Code *of* Law and Code *as* Law' (March 2019), available at https://onlinelibrary.wiley.com/doi/10.1111/1468-2230.12399 (last accessed on 15 November 2019).
[286] Bundesministerium fur Wirtschaft und Energie, 'Blockchain-Strategie der Bundesregierung', available at https://www.bundesfinanzministerium.de/Content/DE/Pressemitteilungen/Finanzpolitik/2019/09/2019-09-18-PM-Block-Anlage.pdf?__blob=publicationFile&v=6 (last accessed on 23 October 2019), p.15.
[287] Ibidem.

strategy can be read as requesting that all smart contracts be stored in a single database.[288] This is a requirement that Member States should ponder carefully as if all other Member States followed suit, there is a risk that the cross-border circulation of smart contracts would be severely limited with the consequence of stifling innovation in the Digital Single Market.

It is worth noting that smart contracts may also present potential opportunities from a consumer protection perspective, such as in InsurTech where they are used to provide automatic compensation to policyholders where flights are delayed.[289] Smart contracts may accordingly lead to more efficient consumer rights enforcement.[290] This potential has not gone unnoticed as the German government has set out to evaluate smart contracts in relation to consumer contracts .[291] Smart contracts thus offer the hope of more efficient enforcement of law through technology.[292]

Consumer protection-related considerations may also be the reason for introducing the requirements for the smart contracts to acquire a prescribed form or to comply with certain formalities. The specific features of such required formalities and the consequences if these requirements are not met differ in various jurisdictions, yet they could include for instance the obligation for the contract to be in writing, to be delivered / stored in a particular way. The rationale behind such requirements could be to be used as evidence, information or to provide a warning, therefore also to be used for consumer protection purposes. Equally, in relation to consumer protection laws, notifications to consumers often need to be provided in a form of text that is sufficient to inform or warn consumers.[293]

Consumer protection related reasons may also play a role when determining the law governing a given contract. While in general the courts would uphold the parties' express choice of law governing a contract (including a smart contract),[294] this might not be the case if consumer protection considerations come into question. Mandatory overriding provisions may namely apply to contracts involving a consumer located or habitually resident in that jurisdiction, regardless of the governing law of the contract. Such mandatory provisions may include consumer protection laws (e.g., distance selling requirements), data protection laws or laws relating to general terms and conditions.[295]

---

[288] Ibidem, p.15 (So kann das Register Anwendern und Entwicklern bei der Ausgestaltung von Smart Contracts unterstützen, da auf ähnliche Anwendungsfälle zurückgegriffen werden kann. Dabei soll das Smart-Contract-Register in der Energiewirtschaft exemplarisch für andere Wirtschaftssektoren stehen und als Basis für die Ausgestaltung und den Aufbau weiterer Register stehen').

[289] In this scenario, the smart contract is connected to global air traffic databases and where these reveal a delay exceeding a pre-determined threshold, compensation is provided directly to the consumer; 'AXA goes blockchain with fizzy' (13 September 2017), https://www.axa.com/fr/newsroom/actualites/axa-se-lance-sur-la-blockchain-avec-fizzy (last accessed on 23 October 2019).

[290] Martin Fries, 'Law and Autonomous Systems Series: Smart consumer contracts - The end of civil procedure?' (March 2018), Oxford Business Law Blog, available at https://www.law.ox.ac.uk/business-law-blog/blog/2018/03/smart-consumer-contracts-end-civil-procedure (last accessed on 23 October 2019).

[291] 'Koalitionsvertrag zwischen CDU, CSU und SPD' (12 March 2018), n°124, available at https://www.cdu.de/system/tdf/media/dokumente/koalitionsvertrag_2018.pdf?file=1 (last accessed on 23 October 2019).

[292] This is also explored in relation to tax compliance.

[293] Clifford Chance, 'Smart Contracts: Legal framework and proposed Guidelines for Lawmakers' (October 2018), available at https://talkingtech.cliffordchance.com/en/emerging-technologies/smart-contracts/smart-contracts--legal-framework-and-proposed-guidelines-for-law.html (last accessed on 18 December 2019).

[294] Article 3 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 Regulation); Article 14 the Rome II Regulation (Regulation 864/2007/EC) (for non-contractual obligations within its scope of application).

[295] Clifford Chance, 'Smart Contracts: Legal framework and proposed Guidelines for Lawmakers' (October 2018), available at https://talkingtech.cliffordchance.com/en/emerging-technologies/smart-contracts/smart-contracts--legal-framework-and-proposed-guidelines-for-law.html (last accessed on 18 December 2019).

One specific element of EU consumer law that is worth highlighting in this context is the right of the consumer to withdraw from the contract and the question of how this can be implemented in relation to smart contracts. Article 9 EU Directive 2011/83/EU on consumer rights foresees that consumers have a right of withdrawal from consumer contracts concluded at a or off-premises without giving a reason, for 14 days. If the trader has not provided the consumer with the information on the right of withdrawal as required, the withdrawal period shall expire 12 months from the end of the initial withdrawal period.[296] If the trader has provided the consumer with the information on the withdrawal right within 12 months from the day of the conclusion of the contract (in case of provision of services contracts) or coming into possession of goods, the withdrawal period shall expire 14 days after the day upon which the consumer receives that information.

However, Article 16 of Directive 2011/83/EU also provides for exceptions from the right to withdrawal. In accordance with Article 16(a) of the Consumer Rights Directive, the right to withdrawal does not apply in relation to 'service contracts after the service has been fully performed if the performance has begun with the consumer's prior express consent, and with the acknowledgement that he will lose his right of withdrawal once the contract has been fully performed by the trader'. In those cases where there is a service contract, and the consumer expressly consents to a restriction to her right of withdrawal, the right to withdrawal no longer applies once the service has been fully performed. This may apply in some circumstances where smart contracts are used. In those scenarios where smart contracts are used that do not fall within the scope of this (or another exception in Article 16 GDPR) traders will nonetheless need to make sure that consumers' right to withdrawal can be respected. It is thus incumbent on traders using smart contracts that this is indeed the case.

3.3.1.4. Smart contracts and pseudonymity

Pseudonymity is a characterizing feature of blockchains and smart contracts. In these systems, users are usually identified by a so-called public key (essentially a string of letters and numbers) that does not directly reveal a user's identity but generally does so where matched with additional information. These identifiers accordingly qualify as pseudonymous.

Pseudonymity presents advantages and disadvantages from a legal perspective. From the perspective of data protection and privacy it can be beneficial (where the public key relates to a natural person as opposed to a firm) as it offers higher protections. However, pseudonymity may also burden compliance with other areas of the law, such as Anti-Money Laundering legislation and more generally the prevention and prosecution of crime as it is more burdensome to detect the real identity behind a pseudonym.[297] Furthermore, for the parties to the contract themselves, redress in court can be an issue as it may be difficult to identify the counterparty.[298]

Some have worried whether pseudonymity may hinder contract formation where blockchain-based smart contracts are intended to be used to this effect. As a starting point, it ought to be stressed that not all national contract law regimes require that the identities of the parties always be known. Indeed, German law does not always require

[296] Article 10, 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 Text with EEA relevance, *OJ L 304,* 22 November 2011, p.78.
[297] Op.Cit., Report of the EU Blockchain Observatory and Forum, 'Legal and Regulatory Framework of Blockchains and Smart Contracts', p.23.
[298] Elise Melchior, 'Réflexions juridiques autour de la blockchain: analyse sous l'angle du droit des contrats' (2019), 72, Revue du droit des technologies de l'information° 45, p.58.

identification of the contracting parties.[299] Also in Swiss law, identification is only required in specific circumstances.[300] In English law, there is no explicit requirement regarding the identity of the parties.[301] However, if a party is not identified in the contract, it may pose problems of lack of certainty or completeness. Similarly, if the party is not identified, there may be issues regarding validity of signature. In order to be enforceable, the contract needs to be entered into by a legal or natural person, and some sort of consideration needs to be provided by a legal or natural person. Traditionally, this consideration needed to move from the promise, so that unless the promisee is identifiable, it is difficult to see how he can enforce (as it cannot be shown that the promisee has provided consideration). Moreover, in cases of mistaken identity (i.e. where a party believes they are contracting with someone else) it is established that where the identity of the person mattered to the contract and the mistake concerns identity not attribute the contract may be held to be void ab initio (i.e. it never existed in the first place).[302] However, there does not seem to be jurisprudence dealing with a lack of identity of a party to the contract. It would seem that, provided the parties can overcome the problems identified above, a contract between parties whose identity is not known could be found to be valid.

There are, however, specific circumstances where identification is legally required in most jurisdictions. In Germany, paragraph 11 read in conjunction with paragraph 2 of the Anti-Money Laundering Act requires such identification in some contexts. [303] In relation to B2C contracts, French law requires that professionals communicate information related to their identity to the consumer before the conclusion of the contract.[304] In Singapore, the parties to an agreement must be also be identifiable as otherwise, the contract may be unenforceable for lack of certainty. The courts can look to the parties' intentions, judged objectively and with regard to the factual matrix of the contract, to ascertain who the intended parties were supposed to be.[305] Moreover, in Italy, in order for a contract to be valid the identity of the parties needs to be known in relation to written contracts, intuitu persona contracts, namely employment contracts.[306] Article 8-ter, paragraph 2, of the Law 19 February 2019, n. 12, the electronic identification of the parties serves to satisfy the written form requirement of smart contracts. Such identification is made in accordance with a procedure that will be set out by the Agid. For B2C contracts, the consumer must also be informed of the identity of the entrepreneur and the corporate name.[307]

It is important to stress that knowing the identity of the parties can also help with the execution of the smart contract where this requires knowledge of such identities.[308] Indeed, it is difficult to bring an action in court against your counterparty unless you have the necessary details regarding their identity. This underlines that requirements

[299] Legal research questionnaire for Germany.
[300] Alexander F. Wagner, Rolf H. Weber, 'Corporate Governance auf der Blockchain', SZW/RSDA, 1/2017, available at https://www.uzh.ch/dam/bf/persons/employee-assets/wagner_alexander/papers/SZW_1_2017_Wagner_Weber_Published.pdf, (last accessed on 23 October 2019), p.59-64.
[301] Also see: The Lawtech Delivery Panel, 'Legal Statement on Cryptoassets and Smart Contracts', UK Jurisdiction Taskforce (November 2019), available at https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf (last accessed on 18 December 2019).
[302] *Ingram v Little [1961] 1 QB 31; King's Norton Metal Co Ltd v Etridge, Merrett & Co Ltd [1972] 1 QB 198.*
[303] Legal research questionnaire for Germany.
[304] Article L 121-17 of the French Consumer Code (Code de la consommation).
[305] Judgement of 14 June 2013, *Derek Hodd Limited v Climate Change Capital Limited*, EWHC 1665 (Ch).
[306] Legal research questionnaire for Italy.
[307] Articles 60 and 97 of Consolidated text of the General Consumer and User Protection Act and other supplementary laws passed by Legislative Royal Decree 1/2007 of 16 November 2007.
[308] 'Smart Contracts: Rechtliche Voraussetzungen und Herausforderungen' (Smart Contracts: Legal requirements and challenges), available at: https://www.srd-rechtsanwaelte.de/blog/smart-contracts-recht/ (last accessed on 23 October 2019).

for identification, such as in the consumer contracts example above, are motivated by important public policy considerations – here consumer protection – that do not disappear where blockchain is used.

Thus, whereas there are various legal requirements that require the identification of parties to a contract, it is not entirely clear whether these risk unduly stifling the development of smart contracts, Indeed, some have stressed that in reality, this is seldom a problem since parties usually do not access a blockchain directly but through intermediaries, that in fact require verification of their identity.[309] For example, if a buyer purchases blockchain-based tokens through a cryptoasset trading platform, then this intermediary can undertake AML verifications. As a result, even if the identifications on-chain remain themselves pseudonymous, nothing stands in the way of regulatory compliance. This is particularly important in the context of proof-of-stake blockchains. Tokens within these ecosystems cannot be mined and thus must be purchased initially over exchanges which are required to execute KYC/AML checks. Putting the burden of KYC on these intermediaries would significantly improve the options for compliance in other parts of the system – particularly in the operations of staking infrastructure providers.[310] It has moreover been stressed that developing digital identity systems can be a very useful component of blockchains.[311]

The above overview has accordingly revealed that the same limitations that apply to ordinary semantic contracts regarding the identification of parties to a contract also apply to smart contracts. These could be seen as a risk of fragmentation in the Digital Single Market. Yet, in both cases, requirements of identification strive to achieve important policy objectives. As such, it is not clear that these rules impact smart contracts is a disproportionate manner. However, it is worth further exploring the potential of SSI solutions in this respect.

3.3.1.5. Smart contracts and jurisdiction

Blockchains are useful to coordinate actions between a variety of different actors that may be established in various different jurisdictions. This inevitably leads to questions regarding applicable law. For example, the EU Blockchain Observatory and Forum has stressed that 'because blockchains can be both decentralised and global, it can be difficult to ascertain which jurisdiction applies to a blockchain platform. This is of course also the case with digital assets issues on such platforms'.[312]

As already noted above, it can be difficult to determine what precise rules apply in respect of cross-border transactions that involve consumers, certain consumer rights have been harmonised across all EU Member States (notably by the E-Commerce and Consumer Rights Directives as well as the Distance Marketing of Consumer Financial

[309] Interview with Consensys.
[310] European Blockchain Association, 'Staking Infrastructure Working Group Position Paper' (preliminary draft) (2019).
[311] Clifford Chance and European Bank for Reconstruction and Development, 'Smart Contracts – Legal Framework and Proposed Guidelines for Lawmakers' (September 2018), available at: www.ebrd.com/documents/pdf-smart-contracts-legal-framework-and-proposed-guidelines-for-lawmakers.pdf (last accessed on 23 October 2019) p.9-10; see, e.g., The First House To Be Sold Entirely Through Blockchain (October 2017), available at: https://www.leaprate.com/cryptocurrency/blockchain/first-house-sold-entirely-blockchain/(last accessed on 23 October 2019), and UK's first blockchain property purchase recorded in Manchester (March 2018), available at: https://www.buyassociation.co.uk/2018/03/19/uks-first-blockchain-property-purchase-recorded-in-manchester/ (last accessed on 23 October 2019).
[312] Op.Cit., Report of the EU Blockchain Observatory and Forum, 'Legal and Regulatory Framework of Blockchains and Smart Contracts' (2019), p.23.

Services Directives), Yet, these only provide for minimum standards and it is necessary to look towards national law to determine the exact content of the relevant rule.[313]

It is worth stressing that questions of liability and jurisdictional issues are closely linked as different jurisdictions have different rules and standards in relation to liability arising from contract law. The related splintering of laws has been said to make it nearly unmanageable to offer global solutions as firms need to get specific legal advice in relation to each jurisdiction, which can be very time-consuming and expensive.[314] This highlights the cost of regulatory fragmentation, which can be detrimental for the Digital Single Market.

Where blockchain nodes span multiple jurisdictions, jurisdictional questions abound.[315] Where smart contracts are deployed on a blockchain, these jurisdictional challenges also extend to them.[316] One of the key promises of smart contracts is that they reduce transaction costs for parties based in different jurisdictions to add trust and certainty to their business transactions. Yet, in such scenarios it is not evident which law governs the contract. A solution could be for the party deploying the smart contract to specify the governing law and jurisdiction for that contract. Private blockchains may impose specific rules on this issue on their users. Yet, while in principle parties are free to determine questions of competence and applicable jurisdiction, the Rome Regulation (on applicable law) and the Brussels Regulation (on jurisdiction) limit this freedom for consumer contracts.[317] Pursuant to its Article 1, the Rome I Regulation covers almost all contractual obligations in civil and commercial matters. To determine whether the Rome I Regulation also applies it is important to distinguish whether the smart contract is itself a legal contract (which is not always the case) or not. The Rome Regulation will only apply in the first scenario.[318] In that instance, parties may submit their contract to the laws of the jurisdiction of their choice (pursuant to Article 3) even if there is no territorial link to that jurisdiction. This principle of party autonomy has been said to offer 'much needed legal certainty' to smart contracts deployed on transnational blockchain networks.[319]

In B2B relations, parties determine jurisdiction or the default rule applies in the form of the jurisdiction where the service provider habitually resides.[320] Under the Brussels I Regulation's 'special jurisdiction' provision, either party can moreover be sued in the Member State where the services 'were provided or should have been provided'.[321] In contrast, for a consumer contract, special provisions apply unless there has been a choice of applicable law and prorogation of justice.[322] For this to apply, there must be a contract between (i) a natural person acting for purposes outside their trade or profession (the consumer) and (ii) a person pursuing commercial or professional activities in a Member State of the consumer's domicile or activities directed at that domicile and where the contract falls within the scope of these activities.[323] In this

[313] Interview with Nina Siedler.
[314] Interview with Nina Siedler.
[315] In the context of European data protection law, see: Michèle Finck, 'Blockchains and the GDPR' (2018), 4 European Data Protection Law Review, p.17-35.
[316] Op.Cit., EU Blockchain Forum and Observatory, Report on Legal and Regulatory Framework for Blockchains and Smart Contracts, p.11.
[317] Regulation 593/2008 of 17 June 2008 on the law applicable to contractual obligations (2008), OJ, L 177/6; Regulation 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (2012) OJ, L 351/1.
[318] Op.Cit., Giesela Rühl, 'The Law Applicable to Smart contracts, or much ado about Nothing?'.
[319] Ibidem.
[320] Article 4(b) of the Rome I Regulation. This rule applies irrespective of whether the services provider resides in a EU Member State or not.
[321] Article 7 (1) Brussels I Regulation.
[322] Article 6 of the Rome I Regulation and Section 4 of the Brussels I Regulation.
[323] Ibidem., Article 17(1)(c).

scenario, the dispute is governed by the laws of the consumer's country of residence and the consumer has the choice to bring the related action before the courts of their own jurisdiction or that of the supplier (even if outside the EU). It is worth noting, however, that this protective regime only applies in B2C relations. Otherwise, the relationship falls under the general rules on contracts.[324]

The co-existence of a multitude of different national legal regimes in the EU may make it difficult to determine questions of jurisdiction and applicable law, which in turn could be seen as a risk of fragmentation in the Digital Single Market. However, EU law already has specific legal frameworks designed to deal with related consequences such as the Rome I and Brussels I regimes. It is not apparent that smart contracts generate any novel problems in this respect that would require a bespoke regulatory response.

3.3.1.6. Capacity to contract and the protection of minors

As has been observed above, on DLT, the identity of the relevant participants is not necessarily known. Particularly public and permissionless systems are usually pseudonymous networks in which parties do not necessarily know others' real-world identities. In contrast, contract law sometimes requires that the identity of the contracting parties be known. For example, under English common law a contract may be void where the identity of the counterparty is unknown.[325] Where the counterparty's identity is not known, an aggrieved party may also not know against whom to bring actions in court, which also merits analysis from a consumer protection perspective. Beyond, there may be difficulties in proving the existence of a smart contract in court proceedings where it only exists in digital form on the blockchain.

The legal literature has indicated potential difficulties for smart contracts to comply with requirements regarding the capacity to contract and the protection of minors.[326] For instance, it can be problematic to ensure that when concluding a smart contract all the parties have a legal capacity. This is because as seen above, some smart contracts providers do not check for identity – and relatedly legal capacity as they let anyone create a public key and transact on-chain. The contracting parties to a smart contract are, at a technical level, not legal or natural persons but rather pseudonymous cryptographic public keys which may represent persons, firms or machines.[327] Hence anyone, including persons without legal capacity, could conclude a smart contract without their counterparty knowing that this is the case.[328] This might then be the source of a lack of legal certainty for the counter-party that has concluded a contract as this contract would be void without that party knowing that this is the case. At the same time, this would jeopardise the protective objective behind rules on capacity, which by and large seek to protect individuals from entering into legal agreements without necessarily grasping the full extent of their commitment. Indeed, a typical feature of contract law regimes across jurisdictions is that those of young age are excluded from being able to contract in order to protect them from undertaking obligations the extent of which they may not fully grasp.

Across Member States, there are private law provisions dealing with the protection of minors and legal capacity, which may include prohibitions to enter (certain kinds of) contracts. Examples include paragraphs 104 and following of the German Civil Code or Articles 1145 to 1152 of the French Code Civil. Similar requirements also exist outside of the EU. In Singapore, a party must be at least 18 years of age to contract. A contract

[324] Judgement of the Court of 11 July 2002, *Gabriel*,C-96/00, EU:C:2002:436, available at http://curia.europa.eu/juris/liste.jsf?language=en&num=C-96/00 (last accessed on 18 December 2019).
[325] See, by way of example: judgment of the 22 July 1971, *Lewis v Averay*, 3 All ER 907, EWCA Civ 4.
[326] Eg. Op. Cit., Mateja Durovic, Andre Janssen, p.762-768.
[327] Op. Cit., Mateja Durovic, Andre Janssen, p.768.
[328] Op. Cit., Mateja Durovic, Andre Janssen, p.768.

entered into by a person of unsound mind is valid unless it can be shown that that person was incapable of understanding what they were doing and the other party knew or ought to reasonably have known of the first person's mental incapacity. This also applies to intoxication. A person signing on behalf of a body corporate must be authorised to do so.[329] Similarly, Article 2 Italian Civil Code provides that minors under 18 years of age and the disabled are unable to enter into a contract.[330] If a contract is entered into by person that lacks legal capacity, it is voidable.

These national contract law rules can be difficult to enforce with regard to blockchain-based smart contracts where the parties' identities are unknown.[331] Indeed, if one does not know whether a party lacks capacity or a minor is involved, then it is impossible to determine whether they have capacity to contract. Yet, design choices, such as the involvement of an intermediary of other authority able to verify identity (as with AML and KYC) could provide a solution to this problem. At the same time, cryptographic tools such as zero-knowledge proofs could be used to reliably provide information regarding whether or not a party has capacity to contract without, however, disclosing the exact identity of the party.

Identifying the identity of participants is hence oftentimes unavoidable in order to ensure legal compliance. This could either be done through an intermediary such as a blockchain-based application or a cryptoasset exchange which would be in charge of verifying individuals' identity in view of complying with national contract law rules that require identification. Alternatively, one could also imagine the emergence of such systems at the level of the blockchain itself where appropriate governance designs are given. This could be implemented in private and permissioned networks through governance rules foreseeing procedures to, for instance verify whether a party to a smart contract has legal capacity.[332] This may however be burdened in a decentralised network that lack organised communication channels between the relevant actors – yet solving this is essentially a governance question and hence not impossible.

The modalities of disclosure are also important. Indeed, the transparent disclosure of dates of birth to all network participants, is undesirable from a data protection and privacy perspective. Sophisticated cryptographic techniques, in particular zero knowledge proofs could be helpful to implement this solution in a privacy-safeguarding manner.[333]

In this context, it is also worth returning to the topic of digital and SSI, a topic that was recently also addressed by the Blockchain Observatory and Forum.[334] The concept of SSI is intended to provide users with full autonomy about their identifier and control over how related personal information is shared and used and with whom. The fundamental component which makes it possible is the so-called decentralised identifier

[329] Companies Act (Cap 50), s.25B for directors' authority to bind company; doctrine of agency in relation to other representatives of the company (Tan Cheng Han, SC, *Walter Woon on Company Law*, (Sweet & Maxwell, Revised 3rd Ed, 2009), p.85 – 86.
[330] Article 3 of the Italian Civil Code however also provides an exemption for employment contracts.
[331] Legal research questionnaire for Germany.
[332] Capacity is usually determined by the law of the domicile of each party, not the law of the jurisdiction the contract is subject to (where these diverge).
[333] A zero-knowledge proof is a cryptographic method by which one party can prove to another party that they know a value x, without conveying any information apart from the fact that they know the value x. This can be used to prove that someone is above a certain age without revealing any additional information (unlike the case where a passport is used).
[334] The European Union Blockchain Observatory and Forum, 'Blockchain and digital identity', Thematic Report, available at https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf (last access on 23 October 2019).

(DID).[335] A DID represents the user in a pseudonymous way and is derived from a public key generated on a blockchain or other distributed ledger technologies. Users can create and register their DIDs without the need for a central authority. DIDs serve to create lifetime relationships with others in a decentralised and privacy-preserving manner. Only information that is needed should be disclosed. A popular example is that a verifier does not care about the actual date of birth but only if the user is old enough to use or access a service. By using zero-knowledge proofs, the verifier only sees this information, derived from the date of birth without the person proving their identity needing to reveal their actual date of birth. Such proofs are not implemented in all SSI systems but do provide an option for selective proofs without disclosure of the underlying information.

SSI further faces the challenge to merge the real-world identity closer to the offline world. This should be achieved by integrating verifiable credentials that can be issued to assert personal information to the DID. Credentials could contain any information, depending on the issuer, such as a valid digital ID, an attestation about a relationship like a club membership, or a digital diploma. By gathering such credentials, a user could integrate real-world identity characteristics to the online identity. Trust in these credentials is based on a web of trust, where verifiers can look up public signatures of issuers or may request credentials that prove their credibility.

Compliance might hence be achieved though privacy by design and SSI solutions to provide both authentication and identification without sacrificing privacy. In other words, the solution may be less about preventing such network activity and more about building public infrastructure which requires SSI to work and interfaces with existing compliance regulations.

3.3.1.7. Opacity

In accordance with contract law theory, reasonableness and fairness require that parties have their behaviour determined in part by the justified interests of the counterparty, which can for instance influence information obligations between experts and non-experts. Yet, while traditional paper contracts include operational and denotational semantics, smart contracts only include operational semantics. This is indeed a big difference between smart contracts and semantic contracts.[336] It should be noted that since smart contracts are software expressed in 1s and 0s, their coding 'requires an increased formalisation of the contractual terms'.[337] This gives rise to challenges such as how to express a choice of law clause in computer code. It has been noted that many traditional contracts, such as mortgage contracts, may be just as opaque and hard to understand for the average citizen.[338] What distinguishes computer-coded contracts is that their very form can make them hard to understand, and this irrespective of their respective substance.

This raises the questions of how parties without the necessary technical background can negotiate, draft and adjudicate smart contracts. It is interesting to note that technical solutions to this issue are currently being developed, such as interfaces offering templates and other solutions to facilitate engagement with smart contracts for non-

[335] Credentials Community Group, 'A Primer for Decentralized Identifiers', Draft Community Report (19 Jan 2019), available at https://w3c-ccg.github.io/did-primer/ (last accessed on 23 October 2019).
[336] Primavera De Filippi and Aaron Wright, 'Blockchain and the Law the Rule of Code' (2018), Harvard University Press, available at https://www.hup.harvard.edu/catalog.php?isbn=9780674976429 (last accessed on 18 December 2019), p.174.
[337] Maren K. Woebbeking, 'The Impact of Smart Contracts on Traditional Concepts of Contract Law'(2019), available at https://www.jipitec.eu/issues/jipitec-10-1-2019/4880 (last accessed on 24 October 2019).
[338] Based on feedback received during the workshop (more information on the workshop can be found in the introduction of this report).

technical parties.[339] In addition to such solutions there is a strong need for better user interface design on the technical side. Generally, consumers are capable of understanding finality but do not expect that everyday transactions might be irreversible or that losing a password could result in the irreversible loss of funds in an associated blockchain wallet. One way to address this is education. A number of technical efforts are in development to make interacting with blockchains more understandable for laypersons.[340] These efforts generally attempt to piggyback on existing technologies which users already understand to do key management (plugings, OpenAuth, etc.). Additionally, technical efforts are underway to provide a standardised 'Decentralised Key Management System' which would allow users to recover lost cryptographic keys in a decentralised manner.[341]

3.3.1.8. Smart Contract Arbitration Mechanisms

Smart contracts will inevitably be contested, such as where facts change or parties change their mind, where parties think that they have been wronged by the counterparty or where a smart contract is used in the context of a legal contract but the legal document and the computer code differ (imagine for instance the paper contract requiring that payment is executed at 12pm but the smart contract being coded to execute payment at 12am). In the latter context, there are ongoing discussions as to what ought to prevail: the intention with which the legal paper contract is drawn up or the way in which it is coded in computer language.

In some circumstances, so-called smart contract arbitration mechanisms are used to deal with disputes that may arise in the context of a smart contract's execution.[342] These solutions directly integrate dispute resolution systems into smart contracts.[343] A MultiSig[344] could be used to halt the smart contract's execution in the event of a dispute or unforeseen consequences to call an arbitrator (which could be a traditional arbitration, another party, or even a judge). The parallel legal contract could be equipped with an arbitration clause and the smart contract could integrate an arbitration library that allows to pause, resume and alter the software and which connects the smart contract with human beings.[345][346]

It has been suggested that due to the applicability of the New York Convention, the arbitration mechanisms applicable to smart contracts could be based on transnational rather than national courts which would be a remedy to the issues of the lack of specialisation and choice of jurisdiction problems.[347] Hybrid solutions where a natural language contract is linked to the smart contract might be able to solve this

[339] See, by way of example, OpenLaw: https://openlaw.io/. (last accessed on 24 January 2020).
[340] Metamask: https://metamask.io; Portis: https://www.portis.io (last accessed on 24 January 2020).
[341] 'Decentralized Key management', https://hyperledger-indy.readthedocs.io/projects/sdk/en/latest/docs/design/005-dkms/README.html (last accessed on 24 October 2019).
[342] For an overview, see: Markus Kaulartz, 'Smart Contract Dispute Resolution', in *Martin Fries and Boris Paal (eds) 'Smart Contracts'(2019), Mohr Siebeck,* available at https://www.mohrsiebeck.com/buch/smart-contracts-9783161569104 (last accessed on 24 January 2020), p.73.
[343] See by way of example, Kleros: https://kleros.io/#.
[344] Multi-signature is a digital signature which allows a group of users to sign a single document. Multisignature addresses require another user or users sign a transaction before it can be broadcast onto the blockchain.
[345] See, by way of example, Codelegit: http://codelegit.com/.
[346] An arbitration library is a software package that allows an on-chain process to be paused if a dispute occurs, allows this dispute to be resolved by an off-chain arbitrator and allows for the result to be passed back on chain for execution.
[347] Jake Goldenfein & Andrea Leiter, 'Legal engineering on the blockchain: 'smart contracts' as legal conduct' (2018), Law and Critique, available at https://www.academia.edu/36626586/LEGAL_ENGINEERING_ON_THE_BLOCKCHAIN_SMART_CONTRACTS_AS_LEGAL_CONDUCT?auto=download (last accessed on 24 October 2019), p.9.

conundrum.[348] Such hybrid solutions would however also be likely to pose other – new – questions: such as in relation to creating new bodies of sui generis rules. It could also emerge that they would disproportionately rely on one legal system, such as English law, as it is the case in commercial maritime arbitration.[349] It is also possible that such new solutions would result in limitations to the occurring private legal exchanges, and their extent would also need to be thoroughly examined.[350]

Other solutions could be agreements that in some circumstances a smart contract can be 'overridden' by a new smart contract. Here, the first smart contract executes (due to the irrevocability of blockchain transactions) but a second smart contract is used to reverse or change its effects (such as to reimburse the payment that was wrongfully executed).[351]

Some legal literature indicates that the arbitration mechanisms that are now developed in order to be incorporated into smart contracts are motivated by a desire that the execution of a smart contract reflects its parties' true intent.[352]In order to determine the viability of such mechanisms in the EU, it ought to be enquired whether there is anything that would prevent national rules on arbitration from applying to smart contracts.

An important question that emerges is that of the compatibility of smart contract arbitration tools with requirements regarding arbitration proceedings in national law. Indeed, many jurisdictions impose related requirements, particularly regarding the enforcement of an award. In Italy, parties are free to choose arbitration or courts for settlement of disputes and there does not seem to be anything preventing national rules on arbitration proceedings.[353] This would indicate that there is nothing that would prevent reliance on smart contract arbitration. However, pursuant to Article 825 of the Procedural Civil Code, the requesting party seeking to enforce an award must file an application with the competent court of the place where the arbitration was seated, attaching the original or a certified copy of the arbitration agreement. The court verifies the formal regularity of the award and issues an order which renders the award enforceable. The order maybe be appealed to the Court of Appeal within 30 days. These modalities would hence also need to be respected in relation to the enforcement of smart contract arbitration awards. This indicates that where enforcement is not automated and a party seeks enforcement in national courts, an off-chain element is added to smart contract arbitration.

In Singapore, existing limitations that prevent arbitration proceedings such as public policy limitations from applying to normal written or oral contracts would also apply to smart contracts.[354] Beyond, there is nothing that precludes arbitration proceedings from applying to smart contracts per se. In general, awards made in Singapore are binding

[348] To illustrate, a smart contract could be coded to enforce a particular clause of the paper contract (such as payment) and the paper contract would be hashed to the smart contract to serve as a means of interpretation where arbitration clauses exist and the smart contract and paper contract diverge (for instance due to a bug in the computer code).
[349] Op.Cit., Jake Goldenfein & Andrea Leiter, p.9.
[350] Ibidem.
[351] If contracts are written such that their logic can be updated at a later date or replaced with new logic, claims can be handled in normal courts (or via arbitration), and the contracts in question can be updated to reflect the new requirements. This is different from blockchain to blockchain, but it should be noted that various approaches are being utilised by developers to address this issue at the code level. The technical issues are not impossible to overcome.
[352] Michèle Finck, 'Smart Contracts as a Form of Solely Automated Processing Under the GDPR' (January 8, 2019), Max Planck Institute for Innovation & Competition Research Paper No. 19-01. Available at SSRN: https://ssrn.com/abstract=3311370 or http://dx.doi.org/10.2139/ssrn.3311370 (last accessed on 19 December 2019).
[353] Articles 806 to 840 of the Procedural Civil Code govern arbitration proceedings.
[354] International Arbitration Act (Cap 143A), s.11.

and enforceable.[355] An application must be made to the High Court for leave to enforce the award. Moreover, as Singapore is a signatory to the New York Convention any award made in Singapore should be enforceable in other countries that are signatories to the Convention. Also in this case, the requirement that an application be made to the High Court for leave to enforce the award indicates that smart contract arbitration proceedings cannot be purely digital but rather require that parallel offline conditions be respected. Unless the digital procedure is equipped with mechanisms that allow for this, smart contract arbitration will not be compatible with the law.

Regarding Spain, the Arbitration Act 60/2003, applies to domestic and international arbitration conducted in Spain and enables individuals and companies to enter into agreements to submit to one or more arbitrators any disputes that have arisen or may arise on matters not subject to any legal restrictions. Specifically, only disputes relating to matters with free disposal of the parties can be settled by arbitration.[356] This means that criminal, tax, labour or family matters cannot be submitted for arbitration. Therefore, if the matter of the smart contract is of free disposal of the parties, arbitration proceedings could apply. The arbitration agreement binds the parties to its terms and prevents courts from hearing disputes submitted to arbitration, where invoked by the party concerned as a challenge to the court's jurisdiction.[357] Article 41 of Arbitration Act establishes the circumstances that the applicant shall allege and prove in order to make an application to set aside a final award. In relation to the enforcements of an award, arbitration awards issued in Spain are directly enforceable in similar terms as enforcement of a court judgment. The trial court where the awards are delivered are competent to enforce those awards.[358] Once the enforcement claim has been submitted, and if the requirements are met, the tribunal provides a general order of execution. This again highlights that courts ought to be involved in order for the arbitration award to be enforceable, with the same implications as those mentioned above.

In the United Kingdom, there also does not appear to be anything preventing national rules on arbitration (as set out in the Arbitration Act 1996) applying to smart contracts. Pursuant to Article 45(1) of the Act a court may, on application of a party to arbitral proceedings (upon notice to the other parties) determine any question of law arising in the course of the proceedings which the court is satisfied substantially affects the rights of one or more of the parties. The party which is granted an award by the arbitration tribunal can apply to the court to have it enforced in the same manner as a judgment or order of the court to the same effect. In this instance, bridges between the smart contract arbitration proceedings and Member State courts would again need to be provided.

Whereas our review of national laws has revealed that there are no principled obstacles for smart-contract arbitration proceedings to be used, in some countries some factors were identified which could prevent a fully automatic arbitration mechanism based on smart contracts from being legally viable. In Singapore, while there is nothing per se in the legislation that would prevent the arbitration proceedings to be applied to smart contracts, the usual circumstances that would prevent arbitration proceedings from applying to any contracts apply (e.g. if a dispute cannot be arbitrated because it would be contrary to public policy to do so). Furthermore, in Germany, legal obstacles arise in the area of B2C contracts. This is because if a consumer participates, an arbitration agreement according to paragraph 1031 (5) of the Code of Civil Procedure needs to be contained in a separate document, signed by the parties by hand. In Spain, the Arbitration Act rules that only disputes relating to matters in which the parties have free

[355] International Arbitration Act (Cap 143A).
[356] Article 2 of the Arbitration Act 60/2003.
[357] Article 11 of the Arbitration Act 60/2003.
[358] Article 545(2) of the Civil Law Procedure Act.

disposition pursuant to law can be settled by arbitration. Lastly, in Switzerland, there is no provision that would exempt smart contracts from using arbitration. However, the threshold to uphold an arbitration clause that is solely contained in some smart contract code might be very high.

Moreover, there are – in at least some jurisdictions – rules that require the involvement of state courts in one way or another in order to secure that these arbitration proceedings are lawful or regarding their enforcement. This might be considered as an obstacle to the development of smart contract arbitration proceedings, considering that these limitations risk making the latter less appealing, efficient and fast. However, it is also worth noting that existing limitations in national legislation, including those that prevent arbitration being used in certain matters such as family disputes, were designed to protect important public policy objectives. These objectives to not necessarily disappear just because the dispute resolution process is moved from the analogue to the digital realm. As such, it appears prima facie that current rules apply in a technology-neutral fashion.

There are, moreover, important consumer protection considerations in this domain. In fact, another concern has arisen regarding the practical effect of smart contracts and smart contract arbitration mechanisms. Existing experience with digital forms of dispute resolution has revealed that consumers are likely to always abide by the outcome of such processes and not appeal them in ordinary courts. Whereas such dispute resolution mechanisms can thus be understood as providing a higher degree of the enforceability of existing norms compared to traditional court systems[359] others have also expressed concerns that this might move society away from state-sanctioned law and relatedly the rule of law.[360] Again, these are observations that apply to digitalisation overall and are not necessarily unique to DLT.

3.3.1.9. Notarisation

The act of notarisation – and thereby the notarial profession - is highly relevant from a legal perspective. It can be said that a notary takes on a dual role. Firstly, a notary observes and records the presence or absence of a certain fact as an independent witness. In order to do so, a notary, for example, authenticates and verifies documents and signatures. Secondly, a notary determines and decides on what constitutes 'present reality'. For example, with regard to the sale of a property, the notary will make sure that the parties to the sale are real, the property to be sold is real as well, that the sale does not take place under duress and so forth.[361] Moreover, notaries in many countries are seen as representing public authority, meaning that when they provide a seal, this has the force of that authority behind it. In fact, this can be said to constitute the main difference between smart contracts and the act of notarisation. Although both rely on the security and minimisation of manipulation blockchain technology can provide, notarial acts are executed in a clear legislative framework and are connected to the authority of the state.[362]

Blockchain technology could be used as a database in order to facilitate the first role of notaries. Applying DLT in this manner will mean there will be numerous confirmations of one document or signature by different parties (or validators). Moreover, once data is approved and recorded on a blockchain, it will be very difficult for unauthorised

[359] Interview with John Salmon.
[360] Interview with Nina Siedler.
[361] 'Notarization in Blockchain' (April 2019), https://www.blockchainexpert.uk/blog/notarization-in-blockchain (last accessed on 24 October 2019).
[362] 'Blockchain: Impacts on Notarial Professions' (Oct 2019), https://hackernoon.com/blockchain-impacts-on-notarial-professions-a58245030a3f (accessed on 24 October 2019).

alterations to be made.[363] Thus, adopting blockchains in this manner would allow for a transparent accounting system which could easily be audited.[364] To provide an example of potential use, it is interesting to note that the Swedish government ran a pilot project on using blockchains in the context of its land registry.[365] However, the second role fulfilled by notaries is less likely to be taken over by blockchains, as it cannot (yet) be automated.[366] The verification of, for instance, an absence of duress, would still need to be carried out by the notary, which could then of course register this information on a DLT, just as they could on any other database.

Given that blockchains could provide a useful element in current notarisation processes, some experiments in this domain are currently underway. Estonia, for example, is using blockchain technology (i.e. a blockchain document verification processes) in order to verify and provide access to their financial and health services.[367] Generally, these systems rely on public blockchains, as in light of their governance mechanisms private blockchains can sometimes be changed or shut down by one single party. Moreover, public blockchains are better equipped against outside attacks.[368] In Italy, the National Council of Notaries has also embraced blockchain technology. Notarchain, a project launched in 2017 is a platform that enables the conclusion and certification of contractual acts and agreements, their registration and archiving, easily, quickly, safely and without intermediary expenses. It intends to provide notaries with blockchain-based tools for recording information and documents. At first, the project was based on a 'closed' blockchain, with nodes entrusted to qualified subjects. However, the National Council of Notaries, and its computer company Notartel, are now moving instead towards widespread and open ecosystems, such as that of Bitcoin.[369] Beyond, there are now also private sector initiatives that offer notarisation services.[370] This underlines that DLT might be a useful tool for notaries to carry out their professional obligations which would allow for information to more easily be shared among various actors.

While blockchains might in the future turn out to be a useful element in the overall notarisation process, it has also been noted that current legal requirements around notarisation could prevent digital transactions from being concluded purely through digital means, such as blockchain-based smart contracts. As a matter of fact, various jurisdictions require the involvement of a notary public in order for an agreement to become legally binding. In Germany, the creation of any legal entity that comes with a limitation of liability for partners/shareholders requires the involvement of notaries (some legal entities require a notarisation ('Beurkundung') of the foundation deed; all legal entities providing for a limitation of liability of their partners/shareholders require to be filed with the commercial register which only accepts filings signed in front of a

[363] 'Notarization in Blockchain' (April 2019), https://www.blockchainexpert.uk/blog/notarization-in-blockchain (last accessed on 24 October 2019).
[364] 'Blockchain and the notaries: the services won't be replaced but transformed' (August 2018), https://www.fintechfutures.com/2018/08/blockchain-and-the-notaries-the-services-wont-be-replaced-but-transformed/ (last accessed on 24 October 2019).
[365] Rebecca Campbell, 'Sweden Tests Blockchain Smart Contracts for Land Registry' (June 2016), https://cointelegraph.com/news/sweden-tests-blockchain-smart-contracts-for-land-registry (last accessed on 24 October 2019).
[366] 'Blockchain and the notaries: the services won't be replaced but transformed' (August 2018), https://www.fintechfutures.com/2018/08/blockchain-and-the-notaries-the-services-wont-be-replaced-but-transformed/ (last accessed on 24 October 2019).
[367] 'Notarization in Blockchain' (April 2019), https://www.blockchainexpert.uk/blog/notarization-in-blockchain (last accessed on 24 October 2019).
[368] 'Notarization in Blockchain: Part 1' (Aug 2018), https://medium.com/@kctheservant/notarization-in-blockchain-part-1-a9795f19e28d. (last accessed on 24 October 2019).
[369] Consiglio nazionale del notario, 'Il notario presenta "Notarchain", la Blockchain certificata dei notai e i registri volontari digitali' (Oct 2017), available at https://www.notariato.it/sites/default/files/cs_notarchain_13102017.pdf (last accessed on 24 October 2019).
[370] Interview with Middlesex University / ANEC.

notary ('Unterschriftenbeglaubigung').[371] The same applies for transfer of partnership interest or shareholdings in such entities as well as any dealings with real estate. Such legal acts could thus not be concluded by sole reference to a blockchain but would also need to see the involvement of a notary.

In the United Kingdom, for documents to be notarised, they need to be presented to a notary public who attaches their seal to the document and provides a notarial certificate.[372] Unless the legislature or the approved regulator decided to change the approach by which notaries notarise documents, it is unlikely that notarisation will happen on the blockchain any time soon.[373] A particular issue that has been identified in relation to the UK is that there are some issues around electronic signatures, such as where you wanted to use digitalised equity tokens (equity on a blockchain). Under English law, you cannot transfer shares in private limited company unless share transfer form is used which needs to be stamped by stamp office, which makes it impossible to do the process entirely digitally.[374]

In line with other common law countries, notarisation is less of a frequent requirement in Singapore than in civil law countries. Under the applicable local laws, requirements related to notarisation could be met using a blockchain, in the sense that the electronic records of the information ordinarily required in a notarial instrument could be appended to a blockchain for storage. Electronic signatures could also be appended to the blockchain using unique cryptographic keys issued to each party, witness, and the notary public.

It is worth stressing that there already is secondary legislation in place that aims to make sure that notarisation requirements do not unduly stifle innovation in the Digital Single Market. The recently revised directive on the use of digital tools in company law provides for the online formation of companies. Its Article 13g foresees that Member States shall ensure that the online formation of companies can be carried out fully online, meaning that there is no need for applicants to appear in person.[375] It is up to Member States to lay down rules for the online formation of companies, including documentation requirements. Member States must nonetheless ensure that these documents can be submitted in electronic form. [376] These formalities, which are defined at national level, shall however ensure that there are procedures to verify applicants' identity and whether they have the necessary legal capacity and authority to represent the company[377] This, however, only applies to the types of companies listed in Annex IIA of the directive. [378] As a consequence, in some circumstances Member States may maintain requirements to appear before a notary. Moreover, where justified by reasons of public interest in ensuring compliance with the rules on legal capacity and on the authority of applicants to represent a company, the applicants' physical presence may be requested.[379]

This overview has underlined that whereas blockchains are databases that can be used to make notarial processes more straightforward and efficient, the technology should

[371] Interview with Nina Siedler.
[372] According to Section 3 of the Notaries Practice Rules 2014 (as amended July 2017): "A notary in possession of a valid practising certificate issued pursuant to the Notaries (Practising Certificate) Rules 2012 may issue notarial acts in the public or private forms intended for use in England and Wales and in any other jurisdiction.
[373] According to the Legal Services Act 2007, the Faculty Office of the Archbishop of Canterbury is the "approved regulator" of notaries.
[374] Interview with John Salmon.
[375] Article 13(g)(1).
[376] Article 13(g)(2).
[377] Article 13(g)(3)(a).
[378] Article 13(g)(1).
[379] Article 13(g)(8).

not be seen as an outright danger to the notarial profession. Indeed, various jurisdictions have requirements that mandate the active involvement of notaries public and it is unlikely that these will be replaced by purely technological processes in the near future. These requirements may limit the options of relying on DLT in some instances, however they also apply in a technology-neutral fashion and the underlying public policy objectives are also valid in the context of DLT.

Following our analysis of smart contracts, we now move on to our second use case, namely utility tokens.

3.3.2. Utility tokens

Tokens are data on a blockchain that represents a certain value, right or obligation. They are generated through mining or minting. Mining refers to the automated creation of tokens on the basis of a pre-defined set of rules (as is, for example, the case in Bitcoin) whereas minting refers to the customised creation of tokens (and it should be stressed that customisation can also relate to the legal configuration of the token).[380] Smart contracts are used to transfer tokens from one wallet to another. From a technical perspective, it is worth stressing that those that control the private key control the database entry and that in practice, tokens are often controlled by a smart contract.

From a legal perspective, tokens are a significant development given that they embody certain rights and obligations which in the past would rather have been represented by paper copies and traded as such. Oftentimes, tokens are distributed through a so-called Initial Coin Offering ('ICOs'), a term derived from Initial Public Offerings. ICOs are usually preceded by 'White Papers', which serve purposes very loosely, and broadly, similar to these of a prospectus in an IPO. There are no formal rules in relation to the structure of such a White Paper, yet there are some common practices that came to existence in the past few years. A study conducted in 2018 established that the most common elements observed in an a white paper include a description of how the token will be used, what benefits it will bring to its holders, and how the Blockchain architecture will operate, as well as the track record of the funding team (such as the background of the founder and their experience in building a business) and the issuer's location.[381] White papers are becoming more and more common when conducting and ICO, but there is no evidence that the availability of the white paper has any influence over the successfulness of the subsequent ICO.[382]

ICOs also illustrate that in practice, smart contracts and tokens are often combined. Indeed, tokens are frequently minted in using the ERC20 token standard on the Ethereum blockchain. In this instance, a smart contract is created on the basis of the ERC20 token standard (to determine the number of tokens etc) which is then deployed on the Ethereum blockchain. Buyers then send cryptocurrency (usually Ether) to the smart contract, which as a reaction sends tokens to the wallet from which the cryptocurrency originates.

It is paramount to stress that tokens can have different functionalities depending on the specific use case. For example, some of them have been designed as a form of 'digital money', such as most famously Bitcoin whereas others can represent ownership in a

[380] Markus Kaulartz & Robin Matzke, 'Die Tokenisierung des Rechts' (2019), Neue Juristische Wochenzeitschrift 3278.
[381] S. Howell, M. Niessner, D. Yermack, 'Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sale', European corporate governance institute, Finance Working Paper n. 564/2018, available at https://ecgi.global/sites/default/files/working_papers/documents/finalhowellniessneryermack.pdf (last accessed on 18 December 2019), p.9.
[382] Op.Cit, Filippo Annunziata, "Speak, if you can. What are you? An alternative approach to the qualification of tokens and Initial Coin Offerings", p.13.

digital or real-world asset. Again, other classes of tokens have been fashioned in order to grant access to a particular service. In many cases, tokens also combine multiple functionalities, in this case one often speaks of 'hybrid' tokens. Indeed, it has been stressed that 'utility tokens tend to have a hybrid nature and often combine elements of equity or payments tokens as well'.[383]

Policy makers are trying to understand the different functionalities of tokens and which functionality may turn a token into a security prone to regulations.[384] Indeed, depending on how a token is classified, regulatory obligations differ. For instance, where a token classifies as a security, issuers must abide by securities regulation. It is accordingly of utmost importance for token issuers and for enterprises using tokens commercially to determine whether their token qualifies as a security, financial instrument or method of payment. To date, no comprehensive guidance on this matter has been issued at EU level.[385]

Because tokens can be fashioned with various functionalities, there is large agreement that it makes little sense to classify all tokens alike as a matter of law. To reflect such diversity, different taxonomies of tokens have been suggested that usually classify tokens in accordance with their respective functionality. For example, FINMA in Switzerland distinguishes between payment, asset and utility tokens whereas the UK Cryptoassets Taskforce has distinguished between security, exchange and utility tokens.[386] Adopting such a functional approach, many consider that there is a separate category of the 'utility token'. An early adopter of such terminology has been the Swiss FINMA, which considers that utility tokens are 'are tokens which are intended to provide digital access to an application or service'.[387] According to ESMA's SMSG utility tokens 'are intended to provide access to a specific application or service but are not accepted as a means of payment for other applications'. [388] Utility tokens are understood a slightly broader manner by the International Token Standardization Association (ITSA), which includes within this term also access tokens, governance tokens, settlement tokens and ownership tokens.[389] It defines utility tokens as being 'intended to provide a certain sort of utility or right to the token holder within a clearly specified environment (e.g. decentralised network, third-party ecosystem, business relationship or jurisdiction'.[390]

Utility tokens are accordingly designed to convey functional utility or rights to token holders that goes beyond them serving as a means of payment. They typically enable access to a specific service or good (similar to a voucher) that is often provided on a specific DLT platform (as there is currently a lack of interoperability of utilities across platforms). Utility tokens can also represent voting rights. Utility tokens make a specific product or service often provided using a DLT platform accessible. However, due to a

[383] Jones Day, 'ICOs and Token Regulation from a German Perspective' (Oct 2018), https://www.jonesday.com/en/insights/2018/10/icos-and-token-regulation-from-a-german-perspectiv (last accessed on 18 December 2019).
[384] Op.Cit, Filippo Annunziata, "Speak, if you can. What are you? An alternative approach to the qualification of tokens and Initial Coin Offerings", p.22.
[385] The European Union Blockchain Observatory & Forum, 'Key challenges and barriers for blockchain in the European Union' in *Blockchain Innovation in Europe Report (*August 2018), available at https://www.eublockchainforum.eu/sites/default/files/reports/20180727_report_innovation_in_europe_light.pdf?width=1024&height=800&iframe=true (last accessed on 24 October 2019).
[386] 'Finma publishes ICO guidelines' (Feb 2018), https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/ (last accessed on 24 October 2019).
[387] Ibidem.
[388] Securities and Markets Stakeholders Group, 'Advice to Esma: Own Initiative Report on Initial Coin Offerings and Crypto-Assets', available at https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf (last accessed on 24 October 2019).
[389] ITSA, Setting standards for global token markets, available at https://www.bvi.de/fileadmin/user_upload/Regulierung/Branchenstandards/20190125_-_ITSA_-_Setting_Standards_for_Global_Token_Markets.pdf (last accessed on 18 December 2019).
[390] Ibid.

lack of interoperability, they are not accepted as a means of payment for other products or services.[391] It is, however, also important to note that the category of the utility token is not set in stone. Indeed, the overall class of the utility tokens is often again broken down into various sub-categories such as app tokens, product use tokens or consumption tokens.[392]

Considering that utility tokens are often used to provide access to a service or an infrastructure, they can sometimes be compared to software licences or in-game credits. They also sometimes but by no means always also enable owners to partake in blockchain governance. A typical example of a utility token would be Filecoin, a token which gives its owners the right to use computer storage (and those offering storage are rewarded in Filecoin, which can also be traded on cryptocurrency exchanges). It is worth noting that utility tokens are still created in view of making a profit and that they can also be traded on secondary markets. Indeed, as ESMA has stressed 'utility tokens are often used as investment products.[393]

Utility tokens hence offer different benefits and risks. They also have different approaches to creating utility. A major way to provide utility is by giving access to a digital service similar to a paid API key. Another type of utility tokens is 'work tokens'[394], which provide the right to contribute to a system. The ICO of a utility token often is similar to the crowdfunding sales on various websites.[395] The benefits are said to include that utility tokens representing services 'may facilitate trading in such services and present an alternate source of early stage funding for innovative projects.' Furthermore, they 'also have a business dimension: by issuing those tokens the issuer creates a network of users, which further increases the value of the business'.[396] Concerning the risks of utility tokens, there are counterparty and performance risks as 'the issuer of the token may not deliver the service as expected, or may go out of business, making the token useless'. [397] Beyond, if utility tokens can be traded on secondary markets 'there is a risk of market abuse and potentially the risk of it being actually purchased as a speculative investment'. [398] Beyond, utility tokens may turn out not to be a durable model as their success depends on users being willing to pay for a future service, although that service may not materialise. It may turn out that if 'a free-to-the-consumer alternative exists, that model will be difficult to sustain'.[399]

There is currently some concern that applicable law creates barriers to investing in decentralised systems and related utility tokens, which may stifle innovation and create a competitive disadvantage for the EU. Overall, it appears that this is an area with

[391] EBA Report, 'Report with advice to European Commission on Cryptoassets' (Jan 2019), available at https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf?retry=1 (last accessed 24 October 2019), p.7.
[392] See, by way of example: 'Blokchain Technology-Thoughts on Regulation' (Aug 2018), https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/BaFinPerspektiven/2018/bp_18-1_Beitrag_Fusswinkel_en.html;jsessionid=AA4F226A1806115F3FC4AD10BCB21307.1_cid390 (last accessed on 24 October 2019).
[393] Securities and Markets Stakeholders Group, 'Advice to Esma: Own Initiative Report on Initial Coin Offerings and Crypto-Assets', available at https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf (last accessed on 24 October 2019).
[394] Coins vs. Tokens - The Complete Guide, available at https://jibrel.network/en/blog/blockchain/token-vs-coin/ (last accessed on 24 October 2019).
[395] Filippo Annunziata, "Speak, if you can. What are you? An alternative approach to the qualification of tokens and Initial Coin Offerings", Bocconi Legal Studies Research Paper Series, February 2019, p.22.
[396] Securities and Markets Stakeholders Group, 'Advice to Esma: Own Initiative Report on Initial Coin Offerings and Crypto-Assets', available at https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf (last accessed on 24 October 2019).
[397] Ibidem.
[398] Ibidem.
[399] Ibidem.

lacking legal certainty. This is not so much the case due to lacking regulatory standards (although there is no specific regulation applying to utility tokens at EU level and in many Member States general financial regulation applies) but rather because there is uncertainty as to what classes of tokens fall within the scope of existing regulation. The potentially negative implications of this lacking legal certainty have been highlighted as commentators have observed that 'the lack of a harmonised regulatory framework for ICOs will likely drive entrepreneurs to specific jurisdictions such as Singapore or Gibraltar, which are strategically framing their laws to attract new digital entrepreneurs. These jurisdictions are particularly appealing for ICOs, not only because they provide a more favourable regulatory framework, but also because they come with a lower degree of regulatory uncertainty regarding the extent to which these new fundraising practices might or might not comply with existing laws and regulations.'[400]

To date, particular attention has been paid to the question of whether (utility) tokens qualify as securities. If this is the case, then the whole range of related financial regulations apply. Article 4(44) of the Markets in Financial Instruments Directive ('MiFID2') defines a transferable security as a security which is 'negotiable on the capital market, with the exception of instruments of payment'.[401] Examples that are listed include shares, bonds or other forms of securitised debt and any other 'any other securities giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities, currencies, interest rates or yields, commodities or other indices or measures'.

Under MiFID2 there are three main criteria that allow for a determination of whether a token is a security: (i) transferability, negotiability on the capital market, and (iii) that the unit is defined by common characteristics, meaning that it is possible to refer to the type and number of units to trade them (the 'standardisation' requirement).[402] While a case-by-case analysis needs to be undertaken to determine whether a specific token meets this definition many financial supervisory authorities have stressed that at least some tokens are securities. [403] As a consequence, a number of obligations emerge such as that to issue a prospectus in accordance with the requirements of the Prospectus Regulation, Market Abuse Regulation[404] or certain fiscal obligations. Consideration of the Alternative Investment Funds Directive[405] could also become necessary.

Many however doubt that utility tokens are securities under MiFID as the concept of 'securitised debt' requires that there be a transfer of some sort of financial claim.[406] By and large, most observers agree that pure currency and utility tokens are exempted

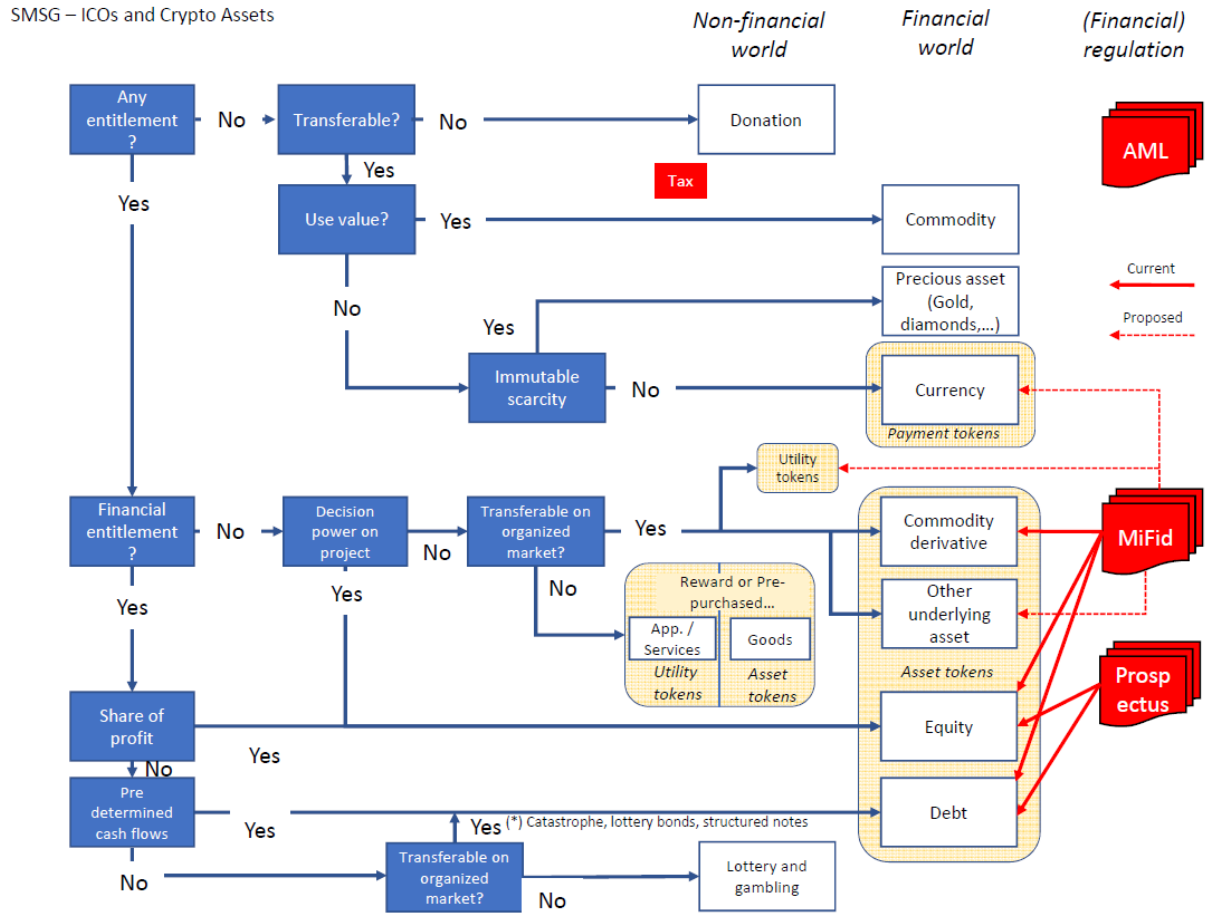
[400] Primavera Filippi, Benedikt Schuppli, Cosntance Choi, Carla Reyes, Nikita Divissenko et al., 'Regulatory Framework for Token Sales: An Overview of Relevant Laws and Regulation in Different Jurisdictions'(Feb 2019), Research Report, Blockchain Research Institute and Coala, available at https://hal.archives-ouvertes.fr/hal-02046797/document (last accessed on 24 October 2019), p.12.
[401] 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 OJ, L 173, p.349–496.
[402] Article 4 MiFID2.
[403] Such as the German BaFin, see: 'Initial coin offerings: BaFin publishes advisory letter on the classification of tokens as financial instruments' (29 March 2018), https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2018/fa_bj_1803_ICOs_en.html (last accessed on 18 December 2019).
[404] Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC Text with EEA relevance.
[405] Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010,OJ, L 174, p.1–73.
[406] Philipp Hacker and Chris Thomale, 'Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law' (Jan 2018), forthcoming in European Company and Financial Law Review, p.20, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820 (last accessed on 24 October 2019).

from securities regulation in the EU.[407] This, does not, however, necessarily mean that they are also exempt from national financial regulation. Indeed, it has been noted that some tokens may not fall under EU securities law but still be caught by national financial regulation in Italy as long as there is an expectation of a financial reward attached to it.[408] As utility tokens are only usable in relation to the issuer, they are not transferable and not covered by MiFID II, the Prospectus Regulation or the Market Abuse Regulation.[409] Indeed, utility tokens do not seem to qualify as securities.[410] As utility tokens do not qualify as financial instruments trading on secondary markets does not require prior authorisation.[411] It is also argued that securities legislation would not be appropriate to cover the legal uncertainties around the utility tokens. The use or consumption of a product internal to the community of token holders is crucial in utility tokens. Information asymmetries will often arise between issuers and buyers. However, these asymmetries typically do not relate to financial, but rather to functionality and consumption risks: hence, securities regulation would not suffice to mandate disclosure of these risks. It is rather a task for consumer law or a specifically designed crypto consumer law.[412] It is the domain of consumer law to cover information duties.[413]

ESMA's Securities Markets Stakeholders Group ('SMSG') concurs that if utility tokens are only usable in relationship with the issuer, and not transferable, they should not be covered by MiFID II, the Prospectus Regulation or the Market Abuse Regulation.[414] However, the SMSG also notes that in some circumstances, utility tokens may be transferable and thus have the potential to become investment tokens. With that in mind the SMSG concludes that it may be worthwhile including them in the MiFID II list of financial instruments.[415] This underlines the importance of a detailed case-by-case analysis in view of legally qualifying each token. The below image depicts relevant criteria to be considered in this respect.

[407] Ibidem.
[408] Based on feedback received during the workshop (more information on the workshop can be found in the introduction of this report).
[409] Securities and Markets Stakeholders Group (SMSG), 'Advice to ESMA: Own Initiative Report on Initial Coin Offerings and Crypto-Assets', available at https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf (last accessed on 24 October 2019), p.14.
[410] Philipp Hacker and Chris Thomale, 'Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law' (Jan 2018), forthcoming in European Company and Financial Law Review, p.20, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820 (last accessed on 24 October 2019).
'By and large, pure investment tokens typically must be considered securities, while pure currency and utility tokens are exempted from securities regulation in the EU'.
[411] Interview with the German Federal Financial Supervisory Authority (BaFin).
[412] Philipp Hacker and Chris Thomale, 'Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law' (Jan 2018), forthcoming in European Company and Financial Law Review, p.20, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820 (last accessed on 24 October 2019).
[413] Ibidem.
[414] Securities and Markets Stakeholders Group (SMSG), 'Advice to ESMA: Own Initiative Report on Initial Coin Offerings and Crypto-Assets', available at https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf (last accessed on 24 October 2019).
[415] Securities and Markets Stakeholders Group (SMSG), 'Advice to ESMA: Own Initiative Report on Initial Coin Offerings and Crypto-Assets', available at https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf (last accessed on 24 October 2019).

Figure 1 - ICOs and Crypto Assets[416]



The argument has been made that as utility tokens do not fall under the MiFID2 regime, a new bespoke legal regime on utility tokens may be required. Such steps have indeed been taken in other jurisdictions. For example, Wyoming has created a legal regime dedicated specifically to utility tokens in 2018, which has the effect of exempting such tokens from securities regulation.[417] In Singapore, the planned Payment Services Act ('PSA') will create a unified and comprehensive body of payment services regulation. It establishes two sets of frameworks, (i) licensing payment services; and (ii) designating payment services that are deemed to be significant. 'Payment services' under the PSA include account issuance services, e-money issuance services, and digital payment token services. Under the PSA, payment services cannot be provided or advertised unless the payment service provider is licensed or exempt. The PSA also provides a legal definition of a 'digital payment token'.[418] This definition of a digital payment token is defined quite broadly and may include utilities tokens. Accordingly, parties who provide

[416] https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf.

[417] Wyoming Bill 70, 'Open blockchain tokens-exemptions', available at https://www.wyoleg.gov/2018/Digest/HB0070.pdf (last accessed on 24 October 2019).

[418] Payment Services Act 2019, s.2 (The PSA defines 'digital payment token' as: *"any digital representation of value (other than an excluded digital representation of value) that: (a) is expressed as a unit; (b) is not denominated in any currency, and is not pegged by its issuer to any currency; (c) is, or is intended to be, a medium of exchange accepted by the public, or a section of the public, as payment for goods or services or for the discharge of a debt; (d) can be transferred, stored, or traded electronically; and (e) satisfies such other characteristics as the Authority may prescribe."*).

digital payment token services using utilities tokens may be required to obtain a license under the PSA.[419] Below, we identify the key legal challenges that have emerged in relation to utility tokens in the European Union.

3.3.2.1. The lack of legal certainty and regulatory fragmentation

An important point is that of legal clarity and certainty. Whereas there are many ongoing debates regarding the regulatory implications of blockchain and potentially the need for new legislation, our research has revealed that a key legal issue is the lack of legal certainty as to how various existing legal frameworks ought to be applied to blockchain use-cases.[420]

It appears that at present, stakeholders frequently feel that it is difficult to determine what a legally compliant use case of a blockchain-based utility token would be. Indeed, many interview partners have stressed the importance of the existing lack of legal certainty in relation to how legal frameworks apply to blockchain.[421] Legal certainty is, however, a central ingredient of innovation and stable economies. A 2019 consultation by the German government confirmed that many stakeholders consider an increase in legal certainty as an unavoidable precondition for a stable development of the token economy.[422]

Relatedly, many stakeholders have underlined the difficulties related to having different definitions and legal obligations applying to the same blockchain use-case across the EU. The absence of uniform definitions also makes common discussions difficult.[423] This has led some to argue that a common European definition would be beneficial.[424] At present, where a company wishes to offer utility tokens across the EU, it needs to evaluate and apply the various national legal frameworks of different Member States.

ESMA's Securities Markets Stakeholders Group concurs that in light of the different approaches adopted by Member States, 'there are very divergent regulatory approaches to cryptoassets. Within the EU this creates an unlevel playing field and hampers the creation of an internal market in this innovative field'.[425] The lack of harmonised regulation may be an issue for the internal market as it may drive entrepreneurs to other jurisdictions 'which are strategically framing their laws to attract new digital entrepreneurs'.[426] Such jurisdictions are particularly appealing 'not only because they provide a more favourable regulatory framework, but also because they come with a lower degree of regulatory uncertainty regarding the extent to which these new fundraising practices might or might not comply with existing laws and regulations'.[427]

[419] Singapore Payment Services Act 2019.
[420] Interview with John Salmon, Interview with Nina Siedler.
[421] Interview with the Swiss Cryptovalley Association.
[422] 'Blockchain-Strategie der Bundersregierung' available at https://www.bundesfinanzministerium.de/Content/DE/Pressemitteilungen/Finanzpolitik/2019/09/2019-09-18-PM-Block-Anlage.pdf?__blob=publicationFile&v=6 (last accessed on 24 October 2019), p.6.
[423] Interview with the Italian Companies and Exchange Commission (CONSOB).
[424] Interview with the German Federal Financial Supervisory Authority (BaFin), Interview with Outlier Ventures, Interview with Gide Loyrette Nouel.
[425] Securities and Markets Stakeholders Group (SMSG), 'Advice to ESMA: Own Initiative Report on Initial Coin Offerings and Crypto-Assets', available at https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf (last accessed on 24 October 2019).
[426] Op.Cit., Primavera Filippi, Benedikt Schuppli, Constance Choi, Carla Reyes, Nikita Divissenko et al., 'Regulatory Framework for Token Sales: An Overview of Relevant Laws and Regulation in Different Jurisdictions'(Feb 2019), Research Report, Blockchain Research Institute and Coala, available at https://hal.archives-ouvertes.fr/hal-02046797/document (last accessed on 24 October 2019), p.121.
[427] Ibidem.

Furthermore, the EU Blockchain Forum and Observatory has also recently stressed the importance of legal certainty for Innovation.[428]

At present, there is thus a high degree of regulatory fragmentation regarding utility tokens across the EU. Many Member States, such as Italy or Spain, have however not adopted specific legislation on utility tokens.[429] The same is true outside of the EU, such as in relation to Singapore or the United States of America.[430] A number of jurisdictions are, however, considering the adoption of bespoke legal regimes on utility tokens. The Italian supervisory authority for securities markets (CONSOB) for instance published a discussion document in March 2019 that proposes a specific regulatory regime for this field.[431] Jurisdictions such as Malta, Switzerland, Lithuania, Jersey and the Isle of Man have 'legislated or specifically developed methodologies, criteria or guidelines for assessing how and to what extent ICOs could be considered as financial instruments'.[432] In the United States, the Wyoming Utility Token Act was passed in 2018 and the Colorado Digital Token Act became effective in 2019 and exempts certain digital tokens from the state's securities registration requirements. Similarly, in Malta, utility tokens do not fall within the scope of the new Virtual Financial Assets Act.[433]

Some examples of definitions of 'utility tokens' are provided in the table below.

Table 2 – Examples of definitions of 'utility tokens'

United States: Wyoming Utility Token Act (2018)	Provides an exemption for tokens with specified consumptive purposes that do not provide token owners with a share of the token issuer's profits. More specifically, a token must (i) primarily be used for consumptive purposes; and (ii) not be marketed to the initial buyer as a financial investment, among other requirements. Accordingly, tokens meeting the requirements of the Act do not constitute securities and are more properly classified as intangible property under Wyoming law.[434]
United States: Colorado Digital Token Act (2019)	Exempts certain digital tokens from the state's securities registration requirements. Similar to the Wyoming act, the definition of digital token in Colorado's act includes a 'consumptive purpose' element. The offer and sale of the digital token will be exempt from the registration requirements in Colorado if the following conditions, among other requirements, are satisfied: 1) The primary purpose of the digital token is a consumptive purpose; 2) The issuer markets the digital token for consumptive purposes and not investment purposes; and either:

[428] Op.Cit., EU Blockchain Forum and Observatory, Report on Legal and Regulatory Framework for Blockchains and Smart Contracts, p.10.
[429] Interview with the Italian Companies and Exchange Commission (CONSOB), Interview with the Spanish National Securities Market Commission (CNMV).
[430] In the US, some members of Congress have pushed for legislation, see interview with United States Securities and Exchange Commission (SEC).
[431] CONSOB, 'Initial Coin Offerings and Crypto-Assets Exchanges, Call for Evidence' (19 March 2019), available at http://www.consob.it/documents/46180/46181/doc_disc_20190319_en.pdf/e981f8a9-e370-4456-8f67-111e460610f0 (last accessed on 24 October 2019).
[432] Securities and Markets Stakeholders Group (SMSG), 'Advice to ESMA: Own Initiative Report on Initial Coin Offerings and Crypto-Assets', available at https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf (last accessed on 24 October 2019).
[433] Chetcuchi Cauchi Advocates, 'Malta Utility Token Offering' https://www.ccmalta.com/malta-utility-token-offering (last accessed on 24 October 2019).
[434] Legal research questionnaire for the US.

	a. the consumptive purpose can be realised at the time of sale; or, b. all of the following are met: (i) the consumptive purpose will be available within 180 days of sale or transfer of the digital token; (ii) the initial buyer is prohibited from reselling or transferring the digital token until the consumptive purpose of the digital token is available; and (iii) the initial buyer provides a clear acknowledgement that the primary intent of its purchase is to use the digital token for a consumptive purpose.[435]
Switzerland: FINMA Guidelines (2018)	The Swiss Financial Market Supervisory Authority FINMA categorises tokens into payment tokens, utility tokens and security tokens. Utility tokens are defined as tokens which are intended to provide digital access to an application or service. However, when utility tokens are not yet ready to be used, they might be regarded as security tokens until the infrastructure is ready. When the market uses utility tokens for payments, they might be simultaneously considered to be payment tokens. The FINMA recently also published a guidance on *stable coins*, which is a collective term used for tokens which are somehow linked to an underlying asset (e.g. such as fiat currency) to minimise price volatility. When tokens are considered pure utility tokens, anti-money laundering regulation is not applicable as long as the main reason for issuing the tokens is to provide access rights to a non-financial application of blockchain technology. However, when utility tokens can be transferred and are designed to be used as means of payments, they will also be considered payment tokens. When utility tokens cannot be used at the time of sale but can only be used for future services, utility tokens are considered to be security tokens at the point of issue.
Malta: Virtual Financial Assets Act (2018)	Defines 'virtual tokens' – effectively term of what the industry calls utility tokens as "a form of digital medium recordation whose utility, value or application is restricted solely to the acquisition of goods or services, either solely within the DLT platform on or in relation to which it was issued or within a limited network of DLT platforms."[436]

The 2018 French Loi PACTE creates a regulatory framework for ICOs.[437] Henceforth, the French Monetary and Financial Code enshrines this optional regime. In line with L.552-4 of the Monetary and Financial Code, issuers may apply for a visa from the French financial regulator, the Autorité des Marchés Financiers ('AMF') prior to any public token offerings. Issuers prepare a document to provide any relevant information about the proposed offering and the issuer. This information document may be in a language other than French as long as it is accompanied by a summary in French. This disclosure

[435] Legal research questionnaire for the US.
[436] 'Virtual Financial Assets', CAP.590, 1st November 2018, available at http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=12872&l=1. (last accessed on 19 December 2019).
[437] Loi relative à la Croissance et à la Transformation des Entreprises (English translation: Business Growth and Transformation Act) available at: https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=F7275D3A90F21B39094DE83BF231EF1C.tplgfr44s_1?cidTexte=JORFTEXT000038496102&categorieLien=id (last accessed on 24 October 2019), the so-called « Loi PACTE » (see in particular 85 Loi Pacte).

statement and promotional communications relating to the offer to the public are accurate, clear and non-misleading, and understand the risks of the offer. It indicates in particular the conditions under which information is provided annually to subscribers on the use of the assets collected.

The AMF checks whether the proposed offer includes the guarantees required of a public offer, and in particular that the issuer of the tokens (i) is incorporated as a legal person established or registered in France; (ii) has put in place means allowing the monitoring and the safeguarding of the assets collected within the framework of the offer.[438] The AMF examines this document and the draft promotional communications intended for the public after the issuance of the visa and the supporting documents for the guarantees provided. It affixes its visa on the information document in the manner and within the time set by its general regulations.

If after issuance of the license, the AMF finds that the offer made to the public is no longer in conformity with the content of the information document or no longer provides the necessary guarantees it may order the termination of any communication concerning the offer of its visa and withdraw its approval under the conditions specified by its general regulations, either permanently or until the issuer satisfies again the conditions of the visa.[439] Where a person disseminates information containing inaccurate or misleading indications concerning the issuance of the visa, its scope or its consequences, the AMF may make a public statement mentioning these facts and the persons responsible for those communications.

It appears that other Member States also ponder the adoption of bespoke utility token regimes. A consultation by the German government revealed that most stakeholders would prefer harmonised EU legislation on tokens that do not qualify as securities. This consultation, however, also revealed that speedy regulatory action is considered of paramount importance, which is why national legislation is evoked as a placeholder until EU legislation can be passed. It appears that the German government considers initiating related legislation in the course of 2019. The goal of this legislation is to ensure investor protection to make sure that issuers need to publish a certain prospectus before a public sale can take place. at the same time, it is expected that this will add further legal certainty.[440]

The FinTech action plan, a European Commission initiative that seeks to make Europe's financial markets more integrated, safer and easier, furthermore foresees that an assessment of the suitability of supranational legislation should be undertaken in respect of ICOs and cryptoassets.[441] Other institutions have started to work on this issue. The European Banking Authority recently released a report on cryptoassets[442] while the European Securities and Markets Authority (ESMA) released a report on ICOs and crypto-assets in 2018.[443] Many national financial supervisors have dedicated task forces

[438] L.552-5 of the French Monetary and Financial Code.
[439] L552-6 of the French Monetary and Financial Code.
[440] Op.Cit, 'Blockchain- Strategie der Budesregierung', https://www.bundesfinanzministerium.de/Content/DE/Pressemitteilungen/Finanzpolitik/2019/09/2019-09-18-PM-Block-Anlage.pdf?__blob=publicationFile&v=6 (last accessed on 19 December 2019) p.7.
[441] Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, FinTech Action plan: For a more competitive and innovative European financial sector, COM/2018/0109 final.
[442] European Banking Authority, Report with Advice for the European Commission on crypto-assets (9 January 2019), available at https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf (last accessed on 24 October 2019).
[443] Securities and Markets Stakeholders Group (SMSG), 'Advice to ESMA: Own Initiative Report on Initial Coin Offerings and Crypto-Assets', available at: https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf (last accessed on 24 October 2019).

and the EU Blockchain Observatory and Forum is planning to make crypto-assets a priority for its upcoming agenda.[444]

The main advantage of a common European regime would be to have a harmonised legal framework applicable throughout the EU and to reduce the currently prevailing legal uncertainty. At present, issuers of tokens have little legal certainty as to whether their product is within the scope of securities laws and their only means of gaining legal certainty is through dialogue with national financial regulators, which is timely and costly.[445] Having one legal framework apply throughout the EU would facilitate cross-border businesses and transactions and could in turn strengthen the EU-based blockchain sector and the Digital Single Market. Furthermore, the creation of a bespoke legal regime would reduce the current lack of legal certainty. The resulting certainty and uniformity could be beneficial for the internal market's overall development.

Whether there is a need for bespoke legislation to address this lacking legal certainty is, however, a matter of debate. It has been suggested that supranational clarification of when cryptoassets may be regarded as financial instruments (and more specifically a transferable security) would already provide clarity for market participants and avoid supervisory arbitrage. [446] In fact, oftentimes the lack of legal certainty is the result of complexity as 'very complex legal structures generally apply to utility tokens'.[447]

Furthermore, there are also disadvantages associated with the adoption of new legislation. As the token economy matures, there is increasing awareness that oftentimes contemporary tokens cannot be classified into neat categories of, for instance, 'security' or 'utility' tokens. Rather, they frequently have a hybrid structure, which burdens their legal classification and the subsequent application of corresponding legal regimes.[448] This has also been stressed by regulators who underline that tokens may display both characteristics of product use tokens and virtual currency or security tokens and this require a more in-depth assessment.[449] How a given token is marketed is important as it will determine the legal regime that applies. In fact, where an issuer 'describes the supposed utility token as also functioning as a means of payment, the token may well be considered to be a unit of account and thus a financial instrument'.[450] Given the disadvantages that come with a new bespoke legal framework, some have expressed doubts as to whether this is the preferable option. Indeed, one of our interview partners stressed that to them it would be preferable to use established civil and financial law as a basis and issue implementation guidelines or amendments where needed (as opposed to an upheaval resulting in a new regime).[451] At the same time, it is, however, also worth noting that these definitional issues are not necessarily insurmountable. Indeed, the regulatory scope of application could be that it applies to tokens not currently covered by another *lex specialis* (such as financial regulation) at EU level.

---

[444] Informal information from Michèle Finck as a member of the Blockchain Observatory and Forum.
[445] Interview with the Nordic Blockchain Association.
[446] Interview with the Spanish National Securities Market Commission (CNMV).
[447] Op.Cit., 'Blockchain Technology- Thoughts on Regulation', available at https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/BaFinPerspektiven/2018/bp_18-1_Beitrag_Fusswinkel_en.html;jsessionid=AA4F226A1806115F3FC4AD10BCB21307.1_cid390 (last accessed on 24 October 2019).
[448] Op.Cit., Report of the EU Blockchain Observatory and Forum, 'Legal and Regulatory Framework of Blockchains and Smart Contracts' (2019), p.23.
[449] Interview with the Federal Financial Supervisory Authority (BaFin).
[450] Op.Cit., 'Blockchain Technology- Thoughts on Regulation' available at https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/BaFinPerspektiven/2018/bp_18-1_Beitrag_Fusswinkel_en.html;jsessionid=AA4F226A1806115F3FC4AD10BCB21307.1_cid390 (last accessed on 24 October 2019).
[451] Interview with the Swiss Cryptovalley Association.

3.3.2.2. Consumer protection (including prospectus requirements)

Suggestions around a bespoke legal regime for utility tokens are oftentimes based on an assumption that they should not be subject to securities regulation as such tokens are not designed as investment instruments. It is, however, imperative to note that even where securities regulation does not apply to a specific token, other legal instruments at national and supranational level will apply, such as e-commerce and consumer protection law, and sometimes also national financial regulation.[452] Indeed, there appears little doubt that tokens that are being offered to consumers online must comply with the corresponding legal regimes.

The Consumer Rights Directive requires that specific information[453] be provided in relation to consumer contracts.[454] Article 5 of the Consumer Rights Directive mandates that the consumer be informed about the main characteristics of the goods and service, the trader's identity, address and contact details, the price and arrangements of the payment, the functionality of digital content and its interoperability with hardware and software that the trader is aware of. Article 5 of the E-Commerce Directive furthermore requires that recipients of a service must be provided with information regarding the name of the service provider, its address, contact details and trade registry entry, and VAT identification number.[455] Operators of internet platforms offering virtual currency tokens as well as the issuers of the virtual currency have to comply with the Directive on Distance Marketing of Consumer Financial Services when marketing and promoting this currency.[456] The Directive imposes the obligation on service providers to provide information to consumers when concluding financial services contracts at a distance. However, the information required varies according on the type of services provided.[457]

Blockchains became well-known to the broader public when the number of ICOs was steeply rising around two years ago. It is nowadays well-known that many of these early ICOs were scams that have had detrimental effects on consumers and investors.[458] More generally, consumer and investors may be overwhelmed by new technologies and struggle to intuitively understand what a smart contract or utility token is and what risks and benefits may realistically materialise. Some indeed consider consumer protection to be the most important regulatory challenge when it comes to utility tokens.[459] In general, our interview partners considered that it was important to safeguard consumer protection as blockchains give rise to new applications and business models.[460]

Beyond general consumer protection concerns that may not look much different for blockchain-based business models compared to others, some specific concerns in relation to this technology have also been identified. For example, consumers are exposed to risk where offerors claim that tokens are tradable on secondary markets but consumers have no entitlement to this or may be forced to have recourse to unregulated

[452] Based on feedback received during the workshop (more information on the workshop can be found in the introduction of this report).
[453] See Recitals 34-36 and Article 5 of the Consumer Rights Directive.
[454] For the definition of a consumer contract, see above.
[455] Additional information must be provided in specific contexts, such as for the regulated professions.
[456] Think BLOCK tank, 'The Regulations of Tokens in Europe, Parts A&B: The Eu legal and Regulatory Framework' (June 2019) available at https://distributed-ledger-consulting.de/wp-content/uploads/2019/08/thinkBLOCKtank-Token-Regulation-Paper-v1.0.pdf (last accessed on 24 October 2019).
[457] Ibidem.
[458] William Foxley, 'Exit Scams Swindled $3.1 Billion FromCrypto Inverstors in 2019: Report' (August 2019), available at https://www.coindesk.com/exit-scams-swindled-3-1-billion-from-crypto-investors-in-2019-report (last accessed on 24 October 2019).
[459] Interview with the Spanish National Securities Market Commission (CNMV).
[460] Interview with the Swiss Cryptovalley Association.

markets.[461] Further risks arise where the underlying program code (such as that of a smart contract) contains programming errors or does not correspond to what is described by the offeror. Whereas similar issues of course arise where other technologies are used, this risk may be more pronounced in blockchain contexts considering their tamper-evident nature which can make it harder to remedy such problems. Unless purchasers are experts, they have no means of verifying this.[462] The risk of losses for the consumers also lies in the risk of loss or theft of the private digital key required for any access to their tokens. The loss or theft of a private key constitutes a significant risk as this is the equivalent to losing access to all of the tokens associated with it. Indeed, the investor and him alone bears the responsibility for the safekeeping of this private key. The area of decentralised key management is a key area of research which may significantly impact the options available for restoring such keys in a trustless manner.

The importance of consumer protection has been confirmed by a 2019 consultation by the German government that stressed that many stakeholders consider the creation of a regulatory framework that at the same time provides legal certainty and provides protection to purchases as a precondition for a positive development of the token economy.[463] Thus, an amendment to the German Banking Act transposing the 5th Anti-Money Laundering Directive into the German legal system will enter into force on 1 January 2020. It provides for a segregation between traditional and cryptoassets (the latter category includes utility tokens). It has been mentioned for some time now that it was important to undergo further steps to ensure better consumer protection, for example with a view to protecting consumers from losing private keys. So far, the protective measures have only been applicable when the custody laws did not apply, and as a result they did not cover utility tokens. This is now bound to change, under the newly introduced definition of utility tokens under the German law.[464]

Nevertheless, tokens still bear huge consumer protection risks across the EU Member States. In 2018, the European Supervisory Authorities (ESAs) published a joint report warning consumers against buying payment tokens without careful consideration.[465] However, it has been underlined that not just payment tokens pose risks to the consumers: following a request by the European Commission to review the current state of EU regulation, the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA) issued reports in mid-January 2019. In the EBA's view, European financial stability is not currently threatened by the use of crypto tokens in light of the relatively low level of activity.[466] However, the EBA also warned of the risks for consumers posed by crypto tokens. Additionally, the EBA suggested the European Commission conduct a cost/benefit analysis regarding an EU regime for crypto tokens,

[461] 'Initial coin offerings: High risks for consumers' (Nov 2017), https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2017/fa_bj_1711_ICO_en.html (last accessed on 24 October 2019).
[462] Ibidem.
[463] Blockchain-Strategie der Bundesregierung, available at: https://www.bundesfinanzministerium.de/Content/DE/Pressemitteilungen/Finanzpolitik/2019/09/2019-09-18-PM-Block-Anlage.pdf?__blob=publicationFile&v=6, (last accessed on 24 October 2019), p.6.
[464] Legal research questionnaire for Germany.
[465] 'Warning ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies', available at https://eiopa.europa.eu/Publications/Other%20Documents/Virtual%20Currencies%20Warning.pdf, (last accessed on 17 December 2019).
[466] It is not clear whether the term "crypto tokens" here also includes utility tokens but arguably it could: According to the BaFin website, in their reports, the EBA and ESMA refer to "crypto assets", for which there is no legal definition. BaFin uses the term "crypto tokens" to refer not only to payment tokens such as bitcoin, but also to investment tokens and utility tokens, 'Crypto tokens remain a risk for Consumers' (28 March 2019), https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2019/fa_bj_1902_kryptowaehrung_en.html (last accessed on 19 December 2019).

stressing the risk regulations at national level may pose for fair competition on a level playing field. In its report, the ESMA came to the conclusion that investors are exposed to considerable risks when crypto tokens are not subject to any regulation and advocated for money laundering regulations as well as disclosure requirements at EU level.[467]

Although utility tokens may not be designed and advertised as such, buyers may nonetheless buy them as an investment. Indeed, the German government recently highlighted that although utility tokens are designed to provide access to digital platforms and/or related rights and services, many purchasers are less concerned with this primary use of the token, and more focused on the prospect of potential financial gain when reselling tokens on secondary markets in the future.[468] The SMSG of ESMA agree that because of the option of resale on secondary markets, utility tokens may be perceived by their purchasers/holders as investment objects similar to securities given their transferability on secondary markets. As a matter of fact, consumer and investor protection concerns arise where utility tokens are traded on secondary market as 'there is a risk of market abuse and potentially the risk of it being actually purchased as a speculative investment'.[469]

Utility tokens can usually be traded on the secondary markets and be used for speculative investment purposes.[470] Therefore, In addition to the risk posed by the lack of regulation regarding crypto tokens, the risk of losses for the investors should also be noted. Tokens are often subject to significant price fluctuations and investors bear the risk of entirely losing their investment. If some offerors affirm that their tokens are tradable on secondary market platforms, investors should nonetheless consider the fact that they have no entitlement to trade on secondary market platforms, which might be unregulated. Therefore, the investors bear a significant risk of not being able to sell their tokens or only sell them at a price that does not meet their expectations.[471]

Furthermore, the complexity of the token models and underlying program codes, including the codes for utility tokens, entail a significant potential for abuse and fraud, as for instance illustrated in the Blockchain strategy of the Federal Government.[472] The offeror might provide incorrect information or the code might contain errors and be vulnerable to manipulation that the investors are not able to assess without an extensive technical knowledge. Moreover, the investor must bear the risk that the documentation of the white paper (determined by the offeror) might be insufficient, incomprehensible or misleading and that might be modified by the offeror at any time. There is also a

[467] 'Crypto tokens remain a risk for consumers' (28 March 2019), https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2019/fa_bj_1902_kryptowaehrung_en.html (last accessed on 19 December 2019).
[468] Op.cit, 'Blockchain-Strategie der Bundesregierung', available at https://www.bundesfinanzministerium.de/Content/DE/Pressemitteilungen/Finanzpolitik/2019/09/2019-09-18-PM-Block-Anlage.pdf?__blob=publicationFile&v=6 (last accessed on 24 October 2019), p.6.
[469] Securities and Markets Stakeholders Group (SMSG), 'Advice to ESMA: 'Own Initiative Report on Initial Coin Offerings and Crypto-Assets', available at: https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf (last accessed on 24 October 2019).
[470] Financial Conduct Authority (FCA), 'Guidance on Cryptoassets' (January 2019), Consultation Paper CP19/3, available at https://www.fca.org.uk/publication/consultation/cp19-03.pdf (last accessed on 19 December 2019).
[471] 'Initial coin offerings: High risks for consumers' (15 November 2017), https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2017/fa_bj_1711_ICO_en.html (last accessed on 19 December 2019).
[472] 'Crypto tokens remain a risk for consumers' (28 March 2019), https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2019/fa_bj_1902_kryptowaehrung_en.html (last accessed on 24 October 2019); 'Initial coin offerings: High risks for consumers' (15 November 2017), https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2017/fa_bj_1711_ICO_en.html (last accessed on 19 December 2019).

higher risk of fraud when the offeror cannot be clearly identified and due to the lack of transparency requirements, it is left up to the consumers to always verify the identity, reputability and credit standing of the token offeror.[473]

The risk of investors losing their investment is increased by the vulnerability of ICOs to be tainted by fraud and money laundering and by the possibility of authorities taking necessary measures against such illegal dealings and the persons involved. In general, investors bear the responsibility to have fully understood the benefits and risks of their investment. [474]

It may be briefly mentioned that blockchains may also be a tool to ensure consumer protection. The idea here is that the transparency inherent to blockchain allows to trace whether legal requirements have been met, for instance in the food chain.[475] Moreover, there are also discussions whether it would be worth tailoring disclosure requirements to the digital nature of tokens themselves.[476] Whereas this may bring a range of advantages, it may also carry disadvantages as the average consumer may be unable to understand such disclosures.

Prospectus requirements
The Prospectus Regulation requires that issuers of securities (and thus also of tokens that qualify as securities such as security tokens) offered to the public or admitted to trading on a regulated market located in or operating in an EU Member State publish a prospectus.[477] The goal of that provision is investor protection as the prospectus is designed to give those purchasing the security relevant information that helps them make informed choices.

Given that the Prospectus Regulation applies only to securities, utility tokens fall outside its scope of application. In practice, token offerings – also for utility tokens – are nonetheless often preceded by the online publication of a so-called 'White Paper' (such as on the website of the issuer, but often these are also distributed on social media and in dedicated chat groups). Formal legal requirements (in addition to those applying anyways, such as unfair competition) could ensure that these publications are drafted in the interest of transparency and the consumer.

It has indeed been suggested that 'the European legislator should take the opportunity to complement the Prospectus Regulation by requiring blockchain-specific information providing answers to, for example, the following questions: How does the decentralised business model work? What is the underlying blockchain technology? Have the relevant smart contracts been audited? Which rights are associated with the tokens? On which secondary markets will the token be tradable, if at all? Which regulatory provisions

[473] 'Crypto tokens remain a risk for consumers' (28 March 2019), https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2019/fa_bj_1902_kryptowaehrung_en.html (last accessed on 24 October 2019).
[474] Ibidem.
[475] Op.cit, 'Blockchain-Strategie der Bundesregierung' available at https://www.bundesfinanzministerium.de/Content/DE/Pressemitteilungen/Finanzpolitik/2019/09/2019-09-18-PM-Block-Anlage.pdf?__blob=publicationFile&v=6 (last accessed on 24 October 2019), p.12.
[476] Philipp Hacker and Chris Tomale, 'Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law' (November 22, 2017). 15 European Company and Financial Law Review 645-696 (2018). Available at SSRN: https://ssrn.com/abstract=3075820 or http://dx.doi.org/10.2139/ssrn.3075820 (last accessed 19 December 2019).
[477] The EU Prospectus Regulation replaces the Prospectus Directive and will be applicable from July 2019.

apply?'[478] Stakeholders have also noted that it would be important for consumer to be better informed about the workings and implications of blockchains.[479]

Where such a requirement is considered, it needs to be specified how a 'prospectus' regime for utility tokens would interact with existing secondary legislation. Indeed, there already are existing information requirements under the EU Consumer Rights Directive[480], the EU Distance Marketing of Consumer Financial Services Directive[481] and the E-Commerce Directive[482] that may apply to token sales. For instance, under Article 5 of the E-Commerce Directive, the service provider needs to provide the service recipient inter alia with the following information: a) the name of the service provider; (b) the geographic address at which the service provider is established; (c) the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner; (d) where the service provider is registered in a trade or similar public register, the trade register in which the service provider is entered and his registration number, or equivalent means of identification in that register; (e) where the activity is subject to an authorisation scheme, the particulars of the relevant supervisory authority. Furthermore, according to Article 10 E-Commerce Directive, the consumers need to be provided with the following information: (a) the different technical steps to follow to conclude the contract; (b) whether or not the concluded contract will be filed by the service provider and whether it will be accessible; (c) the technical means for identifying and correcting input errors prior to the placing of the order; (d) the languages offered for the conclusion of the contract. In addition, Article 3 of the EU Distance Marketing of Consumer Financial Services Directive lists all the information about the supplier (Art 3(1)(1), the financial service (3(1)(2)), the distance contract (3(1)(3)) and redress (3(1)(4)) that the consumer needs to be provided with prior to entering into a contract. Finally, Article 6 of the EU Consumer Rights Directive lists all the information that need to be made available to the consumer in distance and off-premises contracts, such as the main characteristics of the goods or services, to the extent appropriate to the medium and to the goods or services (Art.6(1)(a)); the identity of the trader, such as his trading name (Art. 6(1)(b); and the geographical address at which the trader is established and the trader's telephone number, fax number and e-mail address, where available, to enable the consumer to contact the trader quickly and communicate with him efficiently and, where applicable, the geographical address and identity of the trader on whose behalf he is acting (Art. 6(1)(c)). Clarification in this domain would be helpful as it has been noted that these 'do not apply uniformly to token sales across all Member

[478] JonesDay, 'ICOs and Token Regulation from a German perspective' (October 2018), https://www.jonesday.com/en/insights/2018/10/icos-and-token-regulation-from-a-german-perspectiv (last accessed on 24 October 2019).
[479] Interview with the Norwegian Consumer Council.
[480] 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, *OJ L 304, 22.11.2011, p.64–88,* available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0083 (last accessed on 19 December 2019).
[481] Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC, OJ L 271, 9.10.2002, p.16–24, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002L0065 (last accessed 1on 19 December 2019).
[482] 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, OJ L.178, 17.7.2000, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN, (last accessed on 19 December 2019).

States, with rules varying depending on how the relevant Directives have been implemented into national law'.[483]

Furthermore, the EU Consumer Rights Directive applies certain kinds of contracts concluded between a trader and a consumer.[484] It has a specific regime applicable to distance contracts with consumers. Distance contracts are contracts between a consumer and a trader negotiated and concluded primarily using distance communication. Thus, for irrespective of the specific token classification, token issuers that offer their tokens online will be subject to this regime. The E-Commerce Directive applies to contracts concluded electronically (the 'e-commerce contracts') and imposes specific information requirements where these contracts are concluded with consumers. If the issuer is a business undertaking and the buyer a consumer, tokens will be subject to the Unfair Commercial Practices Directive.

As utility tokens do not typically exhibit features that would make them the same as securities, for instance in the UK they would not be captured in the regulatory regime.[485] However, even though the issuers of tokens may themselves not need to be authorised, certain requirements related to the issuance of the tokens may still be applicable – such as prospectus and transparency requirements. Broadly speaking, the prospectus must provide prospective investors with information to make an informed investment decision and is a legal document for which the issuer has legal liability; it is important that all issuers of tokens work carefully with their legal and financial advisers to fully address the disclosure requirements under the Prospectus regime. [486] Therefore it could be argued that subjecting the utility tokens to a prospectus regime could strengthen protection of the consumers acquiring utility tokens.

On the other hand, however, subjecting commodities such as utility tokens to prospectus obligations like IPOs may, however, be seen as a drastic steps in light of the detailed requirements and high compliance costs associated with such an obligation. With this in mind, alternative transparency regimes may be considered, such as standards to be developed by industry that are then endorsed by regulation. This might eventually result in the provision of more detailed information to consumers, and a right to seek remedies in courts where industry fails to abide by such standards without a copying of a prospectus obligation that may not be suitable in this specific context. Of course, as always with partly self-regulatory efforts, it is of outmost importance to ensure that the defined standards work in the service of consumer interests and are not biased towards industry preferences.

3.3.2.3. Trading on secondary markets

Trading on secondary markets is often identified as a regulatory concern in relation to utility tokens. The resale of tokens on secondary markets is usually possible (regardless of issuers' intentions). This has been the source of a lack of legal uncertainty not because there is no law (general financial regulation applies) but rather because there is

[483] Think BLOCK tank, 'The Regulations of Tokens in Europe, Parts A&B: The Eu legal and Regulatory Framework' (June 2019), available at https://distributed-ledger-consulting.de/wp-content/uploads/2019/08/thinkBLOCKtank-Token-Regulation-Paper-v1.0.pdf (last accessed on 24 October 2019).
[484] 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 , *OJ L 304, 22.11.2011, p.64–88,* available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0083 (last accessed on 19 December 2019).
[485] Financial Conduct Authority (FCA), 'Guidance on Cryptoassets' (January 2019), Consultation Paper CP19/3, available at https://www.fca.org.uk/publication/consultation/cp19-03.pdf (last accessed on 19 December 2019).
[486] Ibidem.

uncertainty as to what classes of tokens fall within the scope of EU financial regulation. Indeed, utility tokens are usually still created in view of making a profit, which raises the question of whether they could qualify as investments. It has moreover been noted that trading on secondary markets may transform a utility token that otherwise does not fall within the scope of financial regulation as a commodity derivative caught by MiFID II.[487] This is noteworthy as it illustrates that trading on secondary markets can change the legal qualification of a token.[488]

The Italian securities regulator (CONSOB) considers that it is necessary to provide information on the risks of market abuse and market manipulation where utility tokens are traded on secondary markets.[489] The Spanish regulator likewise considers that secondary markets should be regulated to avoid market abuse and market manipulation. [490]

One of our interview partners has highlighted that the issues that emerge in relation to resale on secondary markets is not unique to utility tokens by drawing an analogy to stamps. Indeed, although stamps are designed as a utility (to post letters) or as a commemorative souvenir people nonetheless sometimes purchase them as investments, hoping that with time or after a specific event, their value will increase.[491] This highlights that all commodities can be subject to speculation and trading, yet only the derivatives markets are subject to financial oversight, begging the question whether the case can be made that there is something specific to utility tokens that begs such oversight. Others are, however, more cautious, warning that such misunderstandings may pose risks to consumers. Indeed, some stakeholders have stressed the consumer protection risks that may emerge in this regard.[492] For example, it has been argued that 'information asymmetries between investors and issuers makes it difficult for investors to correctly assess the success and risk of projects'.[493]

Particular attention has been paid to the resale of tokens on secondary markets. Here, the Market Abuse Regulation is particularly important.[494] Indeed, ESMA's Securities Markets Stakeholders Group has warned that if there is a secondary market for tokens, there is a risk of market abuse (such as insider dealing and market manipulation) and in relation to utility tokens there is also a risk that these are being purchased as a speculative investment (which could then turn them into a security on the secondary market).[495] If utility tokens were to be considered transferable, they would have the potential to become investment objects. In such a case, risks arise that are very similar to risks on the capital markets (investor protection concerns and market abuse concerns). Some have suggested that it would be useful to include such transferable

[487] Based on feedback received during the workshop (more information on the workshop can be found in the introduction of this report).
[488] Filippo Annunziata, 'Speak If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offerings' (February 11, 2019). Bocconi Legal Studies Research Paper No. 2636561. Available at SSRN: https://ssrn.com/abstract=3332485 or http://dx.doi.org/10.2139/ssrn.3332485 (last accessed on 19 December 2019).
[489] Interview with the Italian Companies and Exchange Commission (CONSOB).
[490] Interview with the Spanish National Securities Market Commission (CNMV).
[491] Interview with John Salmon.
[492] Interview with the Nordic Blockchain Association.
[493] Thijs Maas, 'The Case for Hybrid Tokens' (26 June 2019), available at https://www.lawandblockchain.eu/the-case-for-hybrid-tokens/ (last accessed on 24 October 2019).
[494] Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC, OJ L 173, *12.6.2014,p.*1–61. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0596 (last accessed on 19 December 2019).
[495] Securities and Markets Stakeholders Group (SMSG), 'Advice to ESMA: Own Initiative Report on Initial Coin Offerings and Crypto-Assets', available at: https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf (last accessed on 24 October 2019) p.40.

utility tokens in the MiFID II list of financial instruments as this would also allow to consider secondary markets in such transferable utility tokens as MiFID Multilateral Trading Facilities or Organised Trading Facilities, subject to the Market Abuse Regulation..[496]

Legislation is not, however, the only option in this respect. A transparency regime similar to the one suggested above could be a workable alternative to provide sufficient information to investors on the fact that a trading venue for utility tokens is not subject to the same regulatory oversight as a regulated market. It could be argued that the provision of such a warning by the matching platform would enable consumers to decide whether they accept the risk of market manipulation or not. However, consumers may not be able to fully appreciate the implications of such risk-taking, which is why we ponder the creation of alternative transparency regimes below.

3.4. Conclusion

This chapter examined a range of general legal issues that have emerged in relation to blockchains. It then proceeded to consider a range of legal issues specific to smart contracts and utility tokens. Thereby, the chapter set out the legal issues to potentially be addressed by the policy options which will be introduced in the subsequent chapter.

[496] Ibidem, p.14.

4. Chapter 3 – Outline of policy options

4.1. Introduction

Different policy options could be considered to address the frictions identified in the preceding chapter. After setting out the approach we took in identifying the options, this chapter identifies various possible policy options available to the European Commission.[497] More specifically, the wait-and-see and issuing of guidance approaches are discussed, as are the options of new supranational secondary legislation, the opt-in regime and regulatory sandboxes. Each policy option is introduced descriptively before we move on to outline its respective advantages and disadvantages. Having a clear picture of the available policy options allows us to, in the subsequent chapter, link these options to the legal issues relating to blockchain set out previously.

4.2. Approach regarding policy options

As general-purpose technology, blockchains can be used in many different ways in many different contexts. This explains why a range of regulatory discussions concerning the technology have occurred in recent years. As a general-purpose technology, blockchains can moreover be used in many different ways in many different settings. Accordingly, as underlined by the preceding analysis, it is important to carefully think about specific use cases and what these use-cases imply from the perspective of select legal frameworks. Indeed, there is a broader underlying policy choice that needs to be made in deciding on recommendations, namely between the selection of an overarching horizontal regime regulating all aspects of blockchain, and the option of making adjustments to various regulatory frameworks per issue at stake. As can be seen below, we favour the latter approach. This, since given the breadth of application of blockchain and the various sectors which it is impacting upon, there may not be a one-size-fits-all solution. Indeed, different policy options may be suitable for addressing different aspects of specific blockchain use-cases. What is more, over time it may become apparent that a sector-specific approach may be warranted in some domains.

The above analysis has revealed that overall, there is uncertainty in the blockchain community regarding compliance with existing legal obligations. This is problematic as with new technologies, the manner in which they are adopted depends heavily on the legislative environment which is established. It is often feared that this lack of legal certainty may negatively impact the adoption of the technology and, relatedly, the development of the Digital Single Market. In light of this, a key objective of the various policy options considered in further detail below is to provide legal certainty to those wishing to rely on this technology.

A further overall point that has been identified by the above research is that there is a need to balance consumer and investor protection with the promotion of innovation. [498] There is hope that blockchains can lead to innovative business modes that are beneficial to consumer welfare and the European Union's competitiveness in the digital economy. At the same time, however, concerns have been identified that under some circumstances, reliance on this technology triggers disadvantages from the standpoint of consumer and investor protection. In outlining the various policy options below, we accordingly pay particular attention to how these dual objectives may be achieved.

[497] For a more detailed analysis, see Michèle Finck, 'Blockchains Regulating the Unknown' (July 2018), German Law Journal, vol.19, issue 4, available at https://www.cambridge.org/core/journals/german-law-journal/article/blockchains-regulating-the-unknown/38770CD33494CE55811A546F6FB949B7 (last accessed on 24 October 2019).
[498] Interview with the Italian Companies and Exchange Commission (CONSOB).

Regulations have always struggled to keep up with advances in technology. Indeed, some technologies like the Bitcoin blockchain have chosen not to seek regulatory compliance. One of the other challenges of the blockchain approach, which was also one of its original motivations, is that it reduces oversight. Centralised systems, particularly in financial services, also act as shock absorbers in times of crisis despite their challenges and bottlenecks. Decentralised networks can be much less resilient to shocks, which can impact participants directly, unless careful thought is given to their design. There is thus a strong argument for blockchain applications to work within existing regulatory structures not outside of them, but this means that regulators in all industries have to understand the technology and its impact on the businesses and consumers in their sector.

Below, we outline a series of policy options and examine whether they may be suitable in addressing the challenges identified above. This is followed by a policy matrix, which recalls these various challenges and matches them to the most suitable policy option. We examine the wait-and-see approach, the issuing of regulatory guidance, regulatory sandboxes, as well as the options of new supranational secondary legislation. Each policy option is introduced descriptively before we move on to outline its respective advantages and disadvantages. It will be seen that whereas each approach presents advantages and disadvantages that would need to be carefully balanced by the European Commission. Notwithstanding these respective advantages and disadvantages, it can be seen that some policy options appear more suitable to address given challenges compared to others.

4.3. Policy options

4.3.1. Wait-and-see

In essence, the wait-and-see approach consists of the monitoring of given developments, in this case the emerge and spread of a novel technological approach and related business models while assessing their regulatory implications. Indeed, under the wait-and-see tactic regulators are actively involved with a given topic, here blockchain, but not in view of passing to concrete regulatory steps in the immediate future but rather in order to evaluate whether there is a concrete need for such steps at all. As such, the wait-and-see approach is a sustainable regulatory approach, which bases any concrete regulatory reforms on experience and evidence.

The appeal of the wait-and-see approach in respect of many areas of blockchains' regulatory implications are hard to ignore. Whereas there are now a range of specific applications around utility tokens and smart contracts, it is also evident that these are areas that are still developing both from a technical as well as business and economic perspective. As such, concerns have been raised that it may simply be too early to determine the appropriate content of regulation. The above analysis for instance underlined that there remains considerable confusion and uncertainty regarding both the definition and potential of these blockchain-based mechanisms. This is due in part to the fact that the success of the very infrastructure level (the blockchain) remains contingent on technical improvements, such as for instance in respect of scalability. On the other hand, also the very use cases of smart contracts and utility tokens remain somewhat undefined. In particular in relation to utility tokens it has been observed above that many are sceptical as to whether it is really possible to strictly delimit utility tokens from payment methods or securities as many tokens are indeed of a hybrid nature. Beyond, there is also scepticism as to whether utility token-based business models are really attractive enough to consumers to replace current modes of financing related services, such as through subscriptions or targeted advertising. Indeed, some stakeholders have expressed doubt regarding the long-term usefulness of utility

tokens.[499] This explains why up until now many regulators have chosen to wait and see how this technology and related business models develop before pondering their own interventions. In the past, the European Commission has embraced this approach when it announced in 2017 that it was 'actively monitoring' blockchain technology without taking concrete regulatory steps.[500] The wait-and-see approach presents both advantages and disadvantages.

Advantages: The wait-and-see approach offers a number of benefits, which explains why it has been endorsed in many jurisdictions to date. Indeed, this regulatory strategy provides time for regulators to monitor how given use cases develop before they take any concrete action. Some continue to think that it is too early to think about regulating blockchain use cases through specific regulation considering that the technology and related business models are still developing.[501] This entails that there is a considerable risk that regulatory reform is now initiated on the basis of a certain set of assumptions, such as for instance that it is practically feasible to define and enforce a legal category of the 'utility token' yet that in the future, practice reveals that this is not the case.

During the time period during which the wait-and-see approach is pursued, existing legislation of course continues to apply. Indeed, it has been stressed above that smart contracts and utility tokens do not operate in a lawless space. Rather, the full body of national and supranational secondary legislation applies to them. Examples examined in the previous analysis include, for instance, contract law and consumer protection law. Even though there appears to be agreement that utility tokens do not fall under EU securities regulation, other provisions of EU law, such as competition law including restrictions on unfair commercial practices.[502] The latter would apply in particular where incorrect or misleading information about a token is being distributed. Similarly, it has been amply stressed that national contract law already applies to smart contracts that qualify as legal contracts, and of course, depending on the specific use case and the specific behaviour of related actors any other provisions of the overall legal frameworks, including criminal law apply.

Overall, the main advantage of the wait-and-see approach is hence that it promises to eventually result in better regulatory decisions as regulators are afforded the time necessary to make informed and sustainable decisions.

Disadvantages: A major shortcoming of the wait-and-see approach is its inability to counteract regulatory uncertainty. The above analysis has, however, revealed that in many areas there is (i) a lack of legal certainty as to how to apply a given regulatory framework to a given broad use case of smart contracts or utility tokens, and (ii) a growing fragmentation of the European regulatory framework as more and more Member States are looking into legislation associated with the technology. In order to remedy these shortcomings, which can be detrimental for the development of the Digital Single Market, a more proactive stance compared to the wait-and-see strategy may be needed.

The wait-and-see approach is unable to address these concerns. Indeed, its maintenance of the current status-quo risks aggravating regulatory uncertainty with the

[499] Interview with Fundament Group & Bundesblock.
[500] Luke Parker, 'European Commission "actively monitoring" Blockchain developments' (17 February 2017), https://bravenewcoin.com/insights/european-commission-actively-monitoring-blockchain-developments (last accessed on 24 October 2019).
[501] Elise Melchior, 'Réflexions juridiques autour de la Blockchain: analyse sous l'angle du droit des contrats' (2019),Revue du droit des technologies de l'information,n° 45, p.63.
[502] Op.Cit., EU Blockchain Forum and Observatory, Report on Legal and Regulatory Framework for Blockchains and Smart Contracts, p.21.

risk that companies are discouraged from settling in the EU or offering their products in the internal market or move elsewhere. Rather, what stakeholders consider is needed is a more active stance whereby current points of uncertainty are elucidated. This could bet better achieved through the issuing of guidance, an alternative policy approach that is examined just below. Likewise, continuing the wait-and-see approach at EU level may incentivise more Member States to regulate autonomously, and hence increase regulatory fragmentation and relatedly the cost of legal compliance for actors using these technical tools. Below, the option of new EU secondary legislation is introduced, which may be able to remedy these concerns.

4.3.2. Issue guidance

The issuing of guidance constitutes one option to remedy the currently widely-perceived lack of legal certainty around smart contracts and utility tokens. Various guidance tools are available to regulators, which can undertake mere 'signalling' efforts or publish more formalised guidance.[503] The shared goal of these initiatives is that they provide further information to stakeholders how a given existing legal framework should be interpreted and applied in a given contexts. A key finding of our research has been that many stakeholders consider that this is currently far from clear in relation to a number of national and supranational legal frameworks. Whereas Member States ought to deal with national legal provisions, such as those stemming from domestic contract law, the European Commission should initiate guidance efforts at EU level in relation to supranational law, such as in relation to how the various EU consumer protection instrument ought to be interpreted in relation to select use cases of blockchain technology.

To date, a number of regulators in various jurisdictions have followed the guidance approach. For instance, financial regulators across the world have warned that tokens may qualify as securities and specified how the respective legal frameworks would apply to them.[504] This approach is also being embraced in other areas of EU law as the European Data Protection Board is currently preparing guidelines on how to apply the General Data Protection Regulation to blockchains.[505] This is generally perceived as a laudable and important effort considering the many uncertainties that have arisen concerning the interpretation of multiple provisions of this legal framework in relation to blockchain technology.

Advantages: The issuing of regulatory guidance presents the benefit of speed. Indeed, regulators can relatively quickly (compared to the ordinary legislative procedure) issue public statements that specify how a given legal framework ought to be applied to a given context. As a result, the market is slowly informed about the direction of regulators' approach, also preventing stupefaction when it is formalised through enforcement or maybe follow-up legislative reform. This can reduce regulatory uncertainty, which may lead to more compliance. Indeed, one of our interview partners stressed that in their opinion, the existing Swiss guidance on utility tokens has resulted in less scams and a more positive organisation of these tokens. [506] Similar guidance efforts at EU level could provide the same benefits in terms of European Union law,

[503] On signaling, see Tim Wu, 'Agency Threats' (2011), Duke Law Journal, vol 60:1841, available at https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1506&context=dlj (last accessed on 24 October 2019).
[504] See, by way of example, the warnings for Germany: Op.Cit., 'Initial coin offerings: High risks for consumers' (Nov 2017) https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2017/fa_bj_1711_ICO_en.html (last accessed on 24 October 2019) and the United States, see 'Investor Bulletin: initial Coin Offerings' (July 2017) https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings (last accessed on 24 October 2019).
[505] EDPB Workshop Program 2019/2020, https://edpb.europa.eu/our-work-tools/our-documents/work-program/edpb-work-program-20192020_en (last accessed on 24 October 2019).
[506] Interview with the Swiss Cryptovalley Association.

especially since, as seen above, oftentimes there is legislation in place in relation to a specific legal issue that has been identified but there seems to be a lack of awareness regarding its existence. This would respond to the point identified in Chapter 2 that oftentimes, the issue is not so much a lack of regulation but rather uncertainties on how to apply existing law.[507]

Disadvantages: As soft law, guidelines can, however, also be disregarded or overturned by courts that seem such guidance not to comply with existing regulation. As such they may only be an illusory and temporal remedy to a lack of legal certainty. Moreover, the guidance that is issued may not be followed. For example, in light of the high number of investors investing in ICOs particularly in 2017 and 2018, 'warnings issued by national authorities and ESMA seem to have had insufficient effect'.[508] Regulators choosing this approach thus ought to be aware of its transitional nature and the fact that whereas it may – at least temporarily – solve issues related to a lack of legal certainty, it is likely insufficient where there is a genuine legal gap.

4.3.3. New supranational secondary legislation

Jurisdictions around the world have enacted new legislation as a reaction to the emergence of DLT. Malta and Lichtenstein have adopted rather comprehensive legal frameworks.[509] France has passed its loi Pacte to regulate ICOs and service providers in this area.[510] Luxembourg updated its securities framework to enable the trading of dematerialised securities.[511] Others are also considering revising their applicable laws in the new future. For example, Germany recently announced that it is considering legislation on the public sale of 'certain tokens'.[512] Whereas these are national initiatives relating to given aspects of Member State law, some have also called for legislative reform at European Union level. Considering that Chapter 2 has identified regulatory fragmentation and legal uncertainty as key concerns in relation to smart contracts and utility tokens, supranational secondary legislation could offer a number of advantages.

Advantages: Bespoke supranational secondary legislation would have the potential to remove the existing lack of legal certainty. Such an initiative could clearly specify some points which are currently unclear, such as what qualifies as a utility token and what legal obligations flow from that qualification. This legal certainty may in turn serve to not only stabilise existing business ventures in the European Union but furthermore help attract new blockchain use cases and related companies to the European Union. A further key advantage of new supranational secondary legislation would be the reduction or even removal of regulatory fragmentation in the European Union. In particular in our analysis of utility tokens it has been observed that various Member States are regulating in their respect, which underlines the perceived need for concrete legal reform on this

[507] Interview with Consensys.
[508] Securities and Markets Stakeholders Group (SMSG), 'Advice to ESMA: 'Own Initiative Report on Initial Coin Offerings and Crypto-Assets'', available at: https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf (last accessed on 24 October 2019).
[509] Global Legal Monitor, 'Malta: Government Passes Three Laws to Encourage blockchain Technology' (31 Aug 2018), https://www.loc.gov/law/foreign-news/article/malta-government-passes-three-laws-to-encourage-blockchain-technology/ (last accessed on 24 October 2019); 'Liechtenstein preparing Blockchain Act' (August 2018) https://www.liechtenstein.li/en/news-detail/article/liechtenstein-preparing-blockchain-act/ (last accessed on 24 October 2019).
[510] AMF, 'Vers un nouveau régime pour les crypto-actifs en France'(April 2019), https://www.amf-france.org/Reglementation/Dossiers-thematiques/Fintech/Vers-un-nouveau-regime-pour-les-crypto-actifs-en-France (last accessed on 24 October 2019).
[511] Loi du 1er mars 2019 portant modification de la loi modifiée du 1er août 2001 concernant la circulation de titres, available at http://legilux.public.lu/eli/etat/leg/loi/2019/03/01/a111/jo (last accessed on 24 October 2019).
[512] Op.cit 'Blockchain-Strategie der Bundesregierung' available at https://www.bundesfinanzministerium.de/Content/DE/Pressemitteilungen/Finanzpolitik/2019/09/2019-09-18-PM-Block-Anlage.pdf?__blob=publicationFile&v=6 (last accessed on 24 October 2019).

issue but relatedly also increases legal complexity and costs for actors wishing to offer services that span more than one Member State. The creation of a European directive or regulation could harmonise national regimes, increase legal certainty, and decrease compliance costs for the involved actors.

Disadvantages: Issuing new regulation at an early stage of technical development risks codifying concepts and definitions that subsequently change. Indeed, we have outlined above that whereas many now pursue to classify tokens on the basis of a functional approach, there also is a risk that these classifications prove to be of little use in practice, especially as use cases continue to mature. Many are indeed sceptical that utility tokens can really be used as a separate category given that these often also assume characteristics of means of payment or securities. There is also a risk to regulating as it is difficult to see whether current use cases of blockchains are really here to stay. In relation to utility tokens ESMA has moreover highlighted that such tokens may turn out not to be a durable model as their success depends on users being willing to pay for a future service, although that service may not materialise. It may turn out that if 'a free-to-the-consumer alternative exists, that model will be difficult to sustain'. [513] It is, however, also well-known that regulation can be an important driver of innovation.

Where regulation is the preferred option, a number of options arise. Below, a number of different potential forms of new regulation are introduced, and we debate their respective advantages and disadvantages for the use cases at issue.

4.3.3.1. Possible forms of regulation: self-regulation

Self-regulation has been defined by the European Commission as 'the possibility for economic operators, the social partners, non-governmental organisations or associations to adopt amongst themselves and for themselves common guidelines at European level (particularly codes of practice or sectoral agreements)'.[514] According to Julia Black, it refers to 'the situation of a group of persons or bodies, acting together, performing a regulatory function in respect of themselves and others who accept their authority'.[515]

Self-regulation can be mandated by public authorities or adopted voluntarily. Some consider that the argument for self-regulation in digital contexts is particularly strong as these digital networks can leverage the regulatory nature of code.[516] Computer code creates binding rules that may be known to all and nudge individuals into adopting a certain behaviour. Yet, self-regulation also risks privileging industry interests over those of the wider public and other market participants.[517] It is for this reason that it has been suggested in relation to DLT that self-regulation is 'unlikely to sufficiently resolve the

[513] Securities and Markets Stakeholders Group (SMSG), 'Advice to ESMA: Own Initiative Report on Initial Coin Offerings and Crypto-Assets', available at: https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf (last accessed on 24 October 2019).
[514] European Commission, Interinstitutional Agreement on Better Law-Making [2003], OJ, C 321/01, *31.12.2003, p.1–5 (*para. 22).
[515] Julia Black, 'Constitutionalising Self-Regulation' (Jan 1996) 59, Modern Law Review 24, available at https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1468-2230.1996.tb02064.x (last accessed on 19 December 2019), p.27.
[516] Christopher Koopman et al, 'The Sharing Economy and Consumer Protection Regulation: The Case for Policy Change' (2014), https://www.mercatus.org/publication/sharing-economy-and-consumer-protection-regulation-case-policy-change (last accessed on 24 October 2019).
[517] Luca Belli, Pedro Augusto Francisco and Nicolo Zingales, 'Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police' available at https://www.researchgate.net/publication/321950179_Law_of_the_Land_or_Law_of_the_Platform_Beware_of_the_Privatisation_of_Regulation_and_Police (last accessed on 19 December 2019), in *Luca Belli and Nicolo Zingales (eds), Platform regulations: how platforms are regulated and how they regulate us* (FGV Direito Rio 2017), p.46.

market failures that will ultimately allow illicit and fraudulent uses of decentralised technologies to occur'.[518]

It appears that self-regulation would not be an adequate means of addressing the regulatory objectives in relation to utility tokens that have been identified in this Study. Self-regulation would not have the same hierarchical standing as national legislation that exists and thus be unable to resolve regulatory fragmentation in the Digital Single Market. It is furthermore not clear whether industry would have the right incentives to promote objectives such as that of consumer protection in relation to utility tokens, which have been identified as important policy concerns in this Study.

4.3.3.2. Possible forms of regulation: traditional legislation

Command-and-control regulation, also referred to as top-down regulation, is 'regulation by the state, which is often assumed to take a particular form, that is the use of legal rules backed by criminal sanctions'.[519] The EU's regulatory activity is generally associated with secondary legislation crafted under the ordinary legislative procedure.[520] This ensures that regulation can simple, constant, and predictable and apply in a homogenously applying legislation. Secondary legislation creates uniformity across the EU in preventing a fragmentation of national rules and procedures that may limit market access, elements that are particularly burdensome for smaller players.[521] There are, however, also disadvantages to this approach such as that the rules turn out to be inadequate or difficult to enforce if adopted before technologies and markets had the chance to mature.

Secondary legislation would be a more suitable means of addressing the policy objectives associated with supranational legislation on utility tokens. A directive or regulation could remove fragmentation throughout the internal market and moreover be written in a manner that removes legal certainty. At the same time, it would be important that such regulation be flexible enough to stand the test of time and, in particular, account for the dynamic nature of tokens as indeed the technical and functional characteristics of tokens are likely to continue to change as the technology and related use-cases develop further. Co-regulatory solutions may provide more flexibility in this respect.

4.3.3.3. Possible forms of regulation: co-regulation

Co-regulation has been defined by the European Commission as a 'mechanism whereby an [EU] legislative act entrusts the attainment of the objectives defined by the legislative authority to parties which are recognised in the field (such as economic operators, the social partners, non-governmental organisations, or associations)'.[522] Co-regulation denotes various regulatory techniques whereby 'the regulatory regime is made up of a

[518] Carla Reyes, 'Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal' (April 18, 2016). Villanova Law Review, Vol. 61, No. 1, 2016; Stetson University College of Law Research Paper no. 2016-8. Available at SSRN: https://ssrn.com/abstract=2766705 (last accessed on 19 December 2019).

[519] Julia Black, 'Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a "Post-Regulatory" World' (Feb 2001), 54 Current Legal Problems 103, available at https://www.researchgate.net/publication/30527050_Decentring_Regulation_Understanding_the_Role_of_Regulation_and_Self-Regulation_in_a_'Post-Regulatory'_World (last accessed on 19 December 2019), p.105.

[520] Article 294 TFEU.

[521] For a similar argument in relation to online platforms, see European Commission Staff Working Document, 'A Single Market Strategy for Europe: Analysis and Evidence', SWD (2015) 202 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015SC0100 (last accessed on 19 December 2019), p.6.

[522] European Commission, 'Interinstitutional Agreement on Better Law-Making' [2003,] OJ, C 321/01,31.12.2003, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32003Q1231%2801%29 (last accessed on 19 December 2019), para. 18.

complex interaction of general legislation and a self-regulatory body'.[523] This interplay between the regulator and the regulated explains why it has also been referred to as 'regulated self-regulation'.[524] This collaborative process inherent to co-regulation acknowledges the complex interaction between the State, the market, and technology and reflects the spirit of new governance approaches that emphasise the benefits of involving a large pool of stakeholders in the articulation, execution and oversight of regulation.[525] Public authorities voluntarily involve the private sector in the creation, implementation and enforcement of norms. In doing so, the experiences of prior co-regulatory efforts in the European Union should be accounted for.[526] Again, the approach also has shortcomings such that it risks taking more time and that the process can be overshadowed by specific actors.

Given the dynamic nature of blockchain technology, both from a technical and functional perspective, a co-regulatory regime might thus provide more flexibility to make sure that the regulation that will be adopted will be future-proof. At the same time, care should be had that this regime still accounts for the protection of public policy objectives and ensures the objectives of reducing regulatory fragmentation and uncertainty.

4.3.4. An opt-in regime

More recently, there has also been much discussion regarding the possibility of adopting a so-called opt-in regulatory regime as it has emerged in France under the loi Pacte, as introduced above. In the EU, this is often referred to as a the '28th regime', which denotes the creation of an 'EU framework alternative to but not replacing national rules'.[527] This optional supranational regime exists alongside national rules (instead of replacing them) and gives rise to an option for parties to choose the former as opposed to applicable national law. In a way, it is hence a form of optional harmonisation as it makes available a harmonised set of rules instead of mandatorily replacing national laws.

Advantages: Particularly where no comprehensive frameworks governing utility tokens exists at Member State level, an optional European regime could serve as an alternative. If the right information around this alternative is provided, it could help to decrease the current lack of legal certainty as well as regulatory fragmentation in addition to providing an option for pan-European businesses to only need to rely on one single legal framework. The opt-in regime could also be seen as an exercise in regulatory experimentation as it could be used to test new legal principles for a while, maybe before adopting traditional secondary legislation in the future.

Disadvantages: Depending on the approach adopted, an opt-in regime could also be seen to aggravate the existing lack of legal certainty and fragmentation. Indeed, it could be seen to contribute to fragmentation as it would create an additional legal framework in addition to the swelling number of national initiatives particularly on tokens. Moreover, it could also lead to confusion, particularly for consumers, who may think

[523] Christopher Marsden, 'Internet Co-Regulation' (2011), Cambridge University Press, available at https://assets.cambridge.org/97811070/03484/frontmatter/9781107003484_frontmatter.pdf (last accessed on 19 December 2019), p.46.
[524] Wolfgang Schulz and Thorsten Held, 'Regulated Self-Regulation as a Form of Modern Government'(2004), John Libbey Publishing.
[525] Raymond Brescia, 'Regulating the Sharing Economy: New and Old Insights into an Oversight Regime for the Peer-to-Peer Economy' (2016), vol.95, Nebraska Law Review 87, p.134.
[526] See, by way of example 'The Community of Practice for better self- and co-regulation', https://ec.europa.eu/digital-single-market/en/community-practice-better-self-and-co-regulation-cop. (last accessed on 24 January 2020).
[527] Mario Monti, 'A New Strategy for the Single Market – At the Service of Europe's Economy and Society' available at http://ec.europa.eu/bepa/pdf/monti_report_final_10_05_2010_en.pdf (last accessed on 23 October 2019), p.93.

that general national legal principles apply to them whereas the terms and conditions of a service offering opt for the supranational opt-in regime. This may ultimately be confusing to consumers and investors. Some have also warned of the risk of abandoning technological neutrality when it comes to blockchain and regulation.[528] The German BaFin for instance adheres to the 'same business, same risk, same regulation' model whereby the principles of proportionality and equal treatment based on the rule of law can be upheld. [529] Where an opt-in regime were to be adopted, it would be important to ensure that it respects the principle of technological neutrality.

4.3.5. Regulatory sandboxes

The regulatory sandbox is a technique of regulatory experimentation that has attracted much discussion in recent years. The terminology is a play on the term development sandbox that denotes a safe environment for developers to work on software. In such settings, innovators can test their product or business model while being temporarily exempted from a number of legal requirements. In exchange, these actors are often obliged to operate their business model in a restricted manner, such as through a controlled number of clients or risk exposure, and under close regulatory supervision. The process is designed to allow regulators to observe and learn while providing legal certainty to industry. Some have noted that regulatory sandboxes would be attractive tools when it comes to blockchain use cases.[530]

Projects benefit from more lenient regulatory constraints and close dialogue with agencies. Sandboxing is a tool designed to bring innovations to market more quickly while safeguarding public interest considerations. It has been explored by countries such as the UK,[531] Switzerland[532], Singapore[533], the Netherlands [534] as well as Australia, Canada, Hong Kong and Taiwan.[535] Whereas it was first debuted in the FinTech context, other regulators such as the British Information Commissioner's Office have now also embraced it in other domains such as data protection.[536] Regulatory sandboxes also form part of the EU's FinTech Action Plan according to which they 'take the idea of innovation hubs a step further by creating an environment where supervision is tailored to innovative firms or services. National competent authorities must apply relevant EU financial services legislation. However, these rules include a margin of discretion with

[528] Interview with John Salmon; Op.cit, 'Blockchain-Strategie der Bundesregierung' available at https://www.bundesfinanzministerium.de/Content/DE/Pressemitteilungen/Finanzpolitik/2019/09/2019-09-18-PM-Block-Anlage.pdf?__blob=publicationFile&v=6 (last accessed on 24 October 2019), p.12.

[529] Interview with the German Federal Financial Supervisory Authority (BaFin). Also see 'Blockchain Technology-Thoughts on Regulation' (Aug 2018),https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/BaFinPerspektiven/2018/bp_18-1_Beitrag_Fusswinkel_en.html;jsessionid=AA4F226A1806115F3FC4AD10BCB21307.1_cid390 (last accessed on 24 October 2019)

[530] Interview with Outlier Ventures.

[531] More information about this process can be found online under 'Regulatory Sandbox': FCA, 'Regulatory Sandbox', https://www.fca.org.uk/firms/regulatory-sandbox (last accessed on 24 October 2019).

[532] 'FINMA reduces obstacles to FinTech' (17 March 2016) https://www.finma.ch/en/news/2016/03/20160317-mm-fintech/. (last accessed on 24 October 2019).

[533] 'FinTech Regulatory Sandbox: Introduction,' http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/FinTech-Regulatory-Sandbox.aspx (last accessed on 24 October 2019)

[534] 'More room for innovation in the financial sector' (Dec 2016), https://www.dnb.nl/en/binaries/More-room-for-innovation-in-the-financial%20sector_tcm47-361364.pdf?2018050113 (last accessed on 24 October 2019).

[535] FCA, 'Regulatory Sandbox', https://www.fca.org.uk/firms/innovation/regulatory-sandbox (last accessed on 19 December 2019); 'Fintech Regulatory Sandbox', http://asic.gov.au/for-business/your-business/innovation-hub/regulatory-sandbox/ (last accessed on 19 December 2019); 'Fintech Supervisory Sandbox', http://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech-supervisory-sandbox.shtml.

[536] 'ICO selects first participants for data protection Sandbox' (July 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-selects-first-participants-for-data-protection-sandbox/ (last accessed on 24 October 2019).

regard to the application of the proportionality and flexibility principles embedded in these rules. This can be particularly useful in the context of technological innovation'.[537]

Advantages: The objective of regulatory sandboxes is to foster collaboration between regulators and innovators in order to test a new business model that is not prohibited but simply not foreseen in current regulations. While the resulting guidance is helpful for economic actors that experiment with new technologies, it also allows regulators to make the necessary observations to determine whether regulatory change is required as a consequence of the emergence of new technologies and business models.

Disadvantages: Sandboxes also need to be carefully designed from a consumer protection perspective as consumers may think that they are protection by general consumer protection law whereas the sandbox may provide an exemption from some principles to the relevant company. Sandboxes furthermore ought to be carefully designed as they raise issues of competence and trigger the risk of regulatory picking winners and losers in the market as well as concerns from an equality before the law perspective. These issues ought to be carefully addressed to prevent judicial review and political problems. Recent research has moreover found that the expected advantages of sandboxes often do not materialise.[538] Additionally, it must be noted that sandboxes are not really scalable (as there can only ever be a limited number of participants that benefit from the close contact with regulators).[539] Whereas they can be useful tools for experimentation, they cannot be a broad regulatory strategy for an entire sector.

4.4. Conclusion

After setting out the approach we took in assessing policy options, this chapter provided an overview of the policy options available to the European Commission, including a description of each of the option's advantages and disadvantages. In the subsequent chapter, the suitability of these policy options to address the legal issues regarding blockchain technology identified previously will be assessed.

[537] Communication from the commission to the European parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of Region, 'Fintech Action Plan: For a more competitive and innovative European financial sector', COM(2018), 109/2, available at https://ec.europa.eu/info/sites/info/files/180308-action-plan-fintech_en.pdf (last accessed on 24 October 2019), p.9.

[538] Buckey, Ross P. and Arner, Douglas W and Veidt, Robin and Zetsche, Dirk Andreas, 'Building FinTech Ecosystems: Regulatory Sandboxes, Innovation Hybs and Beyond' (September 2019), UNSX Law Research paper No.19-72, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3455872 (last accessed on 24 October 2019).

[539] Based on feedback received during the workshop (more information on the workshop can be found in the introduction of this report).

5. Chapter 4 – Assessment of policy options in light of the legal issues relating to blockchain technology

5.1. Introduction

This chapter assesses the suitability of the policy options set out in the previous chapter in relation to each of the legal issues regarding blockchain technology identified in previous chapters. Building on the substantive analysis carried out in the preceding parts of the Study, this section discusses policy options in relation to both the general legal issues that have been identified in relation to the technology, as well as the specific legal issues relating to the broad use cases of smart contracts and utility tokens that have been the focus of our legal analysis. The overarching aim of the present chapter is to provide some initial policy options for the Commission that may inspire its future approach. We also discuss the timing of each policy option as part of our analysis in case this is a factor of importance to the Commission.

5.2. Assessment of policy options for legal issues regarding blockchain technology

5.2.1. Responsibility for legal compliance and liability

The preceding analysis has highlighted possible challenges of allocating responsibility in decentralised systems, specifically in relation to responsibility for legal compliance and liability. Our analysis has shown, however, that these challenges are not due to shortcomings of the respective legal frameworks but can rather be overcome where the veil of decentralisation is pierced, and an investigation determines where actual responsibility lies. Indeed, our analysis has shown that the issues discussed in this respect do not so much relate to inadequacies in relation to the respective legal regimes (which are generally Member State laws) but rather to the fact that blockchain systems and specific use cases thereof may not have been designed in view of complying with legal requirements on these points. This is not an issue that is unique to blockchains. Rather, it underlines that legal systems require business models and technical systems to be designed to enable legal compliance and that they have mechanisms to enable action to be taken where this is not the case. It has also been seen that national law enforcement agencies in various jurisdictions have successfully enforced existing law in relation to blockchain projects that failed to be compliant and that a number of blockchain analytics companies assisting them in this task have emerged. Responsibility for legal compliance and liability are thus by no means unachievable where blockchains are used as technical infrastructure, yet the latter must be designed in order to enable this.

As a result, we consider that no specific policy response is needed and recommend that the European Commission adopt a wait-and-see approach in this respect as there are currently no indications that Member State or EU law creates any undue burdens on those using blockchains (that would differ from general legal obligations applicable notwithstanding the specific business model or technology at stake). Of course, if evidence to the contrary were to emerge, the situation would need to be re-evaluated.

Rather, the difficulties that have been encountered so far are questions of technology design on the one hand, and the lack of effective enforcement of existing norms by law enforcement agencies on the other. These two issues can be remedied through stricter enforcement and better design. Firstly, those using DLT in their business models ought to make sure that their usage of the technology occurs in a manner that facilitates legal compliance. This requires that attention is paid to pure questions of technical design (for instance, whether it is technically possible to amend on-chain content on a blockchain) but also to blockchain governance, that is to say the human coordination

processes around the protocol. Indeed, such human coordination is needed to take decisions that are essential to facilitate compliance. Governance ought to be fashioned in a manner that legal liability and responsibility can be attributed, and that related factual consequences can be executed in a manner that complies with legal requirements. It appears that first and foremost this task does not fall on public authorities – rather it is for each entity using DLT to make sure they do so in respect of the law, just as the same obligation exists for other businesses using other technologies. Should the European Commission nonetheless desire to take a steering role in this context, it could initiate coordination efforts among relevant stakeholders which should have as its aim the definition of how technology can be rendered compliant-by-design. Furthermore, governance solutions which ensure that compliance is possible could be devised as our research has indeed highlighted that many stakeholders consider that experience with blockchain governance remains limited and related actors often find it difficult to design appropriate solutions. A particular topic in this respect are public and permissionless blockchains such as Bitcoin or Ethereum, which often operate without prioritising legal compliance. Where there is a clear disregard for the law, enforcement by relevant agencies (examined just below) would be the logical conclusion. However, a lack of compliance does not necessarily have to be the result of a desire to disregard the law but simply of lacking experience of how this could be achieved. Indeed, in these transnational networks, multiple individualUNCITRALs loosely cooperating and designing compliant solutions is highly complex, both due to uncertainties regarding applicable law and inexperience with effective enforcement solutions. Should the Commission consider that the innovation potential of public and permissionless blockchains is such that they require support in spite of these regulatory challenges, it could equally encourage action in this respect, such as through research funding or in encouraging industry stakeholders to devise standards and best practices in this respect.

Secondly, our research has revealed that the lack of compliance and responsibility can also result from insufficient law enforcement. For example, whereas there is broad agreement that many of the ICOs conducted in recent years were in breach of securities legislation, not all projects suspected of having been in breach have been prosecuted so far. Similarly, whereas there is broad agreement that many data controllers using blockchains process personal data in a manner that violates the GDPR, no enforcement action appears to have been taken by supervisory authorities so far. This may generate an impression that the cost of non-compliance can be negligible as it is unlikely that enforcement agencies will take action against a specific actor. Enforcement against those who disregard applicable laws (by the competent national and supranational authorities) would thus increase incentives for compliance as it would be clear from the outset that non-compliance is costly.

Oftentimes, observers feel that blockchain technology is a lawless space as indeed, many legal requirements have in the past been broken (such as those stemming from securities legislation) and such breaches have not necessarily been followed by enforcement, or at least such enforcement has not necessarily been well-publicised. Indeed, it has been stressed that Member States public authorities have measures to tackle liability issues and classic remedy systems could and should apply also to blockchains.[540] Seeking a stronger respect for existing norms may chance such perceptions and in turn lead to higher rates of compliance. Of course, this is something that related enforcement agencies must carefully ponder in light of their enforcement priorities and resources. As regards timing, this can be fast to be implemented as enforcement systems are well-established in the various Member States.

[540] Based on feedback received during the workshop (more information on the workshop can be found in the introduction of this report).

5.2.2. Potential barriers in sectoral (e.g. AML) legislation

In relation to the potential barriers in sectoral legislation examined above, our analysis of Anti-Money Laundering law has highlighted that whereas blockchains may offer a number of benefits for more efficient AML processes, related challenges also arise.

Blockchains may offer many benefits from an Anti-Money Laundering perspective as their record-keeping function may be deployed to facilitate compliance with related legal requirements. At the same time, however, some have noted that some projects using blockchains are designed in a way that burdens such compliance, simply because related processes have not been built into the system, sometimes due to a lack of awareness that this legislation applies to a given blockchain-based project.

Also with respect to AML; ensuring compliance is essentially a governance question (for the actor using blockchain) as well as a question of the effective enforcement of existing regulations (from the public authority perspective) and does thus not require a specific policy response. The first suggestion here would thus be that the European Commission adopt a wait-and-see approach as there currently appear to be no arguments supporting immediate action in this field. Our research has indeed shown that there is nothing per se in AML legislation that makes it impossible for blockchains to comply with this (it is thus a technologically neutral framework). As such, we recommend that the European Commission continues to monitor related developments and potentially address these in the context of the next revision of the AML Directive, if considered appropriate.

Should the Commission nonetheless wish to adopt a more active policy approach in this specific context, it could proactively encourage that blockchain-based AML systems are designed in order to ensure compliance with existing regulation from a technical perspective. Research funding could be made available to explore systems that are compliant-by-design. Similarly, research funding could be made available to better understand and design the human coordination processes in a way that they could also be designed so that legal requirements can be met.[541] Generally, blockchain-based AML solutions involve a multitude of different actors (whether natural or legal persons) which need to coordinate through suitable governance arrangements. One tool that could be further explored here is the adoption of standards terms and conditions or model contracts, a method promoted by the Commission in other areas, to coordinate compliance.[542] Indeed, even though AML legislation appears to operate in a technology-neutral manner and even though some even speculate that in the future DLT could be used as a tool that facilitates compliance with related requirements, many actors using blockchain technology presently seem to be struggling with the transposition of the legislation. The European Commission could initiate industry efforts around the creation of standards terms and conditions or model contracts in order to facilitate compliance. Also, in other domains of the digital economy, these tools have been used to facilitate compliance. Standard contractual clauses between service providers and their customers are used in international personal data transfers.[543] Specifically regarding AML, model contracts could be set up by industry to facilitate the blockchain-based AML solutions many are working on while ensuring that the related sharing of information between numerous actors for AML purposes (which is foreseen in such scenarios) is respected. Regarding timing, this is a policy option that could be initiated straight away

[541] Based on feedback received during the workshop on the importance of governance (more information on the workshop can be found in the introduction of this report).
[542] Also see, 'Communication from the Commission to the European Parliament and the Council - European Contract Law and the revision of the acquis: the way forward', (COM/2004/0651 final), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52004DC0651&from=EN. (last accessed on 24 January 2020).
[543] Standard Contractual Clauses (SCC), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (last accessed on 24 January 2020).

and concluded within a couple of years (or earlier, if agreement on the clauses can be fast) as it does not require legislative intervention.

5.2.3. The protection of fundamental legal principles and mandatory rules

It does not appear that the legal issue of protecting fundamental legal principles and mandatory rules is an area that necessitates a concrete policy response. At present, existing principles appear well-suited to address problems associated with the criminal use of this technology. Whereas blockchains have, like all technologies, been used for illicit ends, the related problems are not necessarily unique to this technology. Indeed, there are no indications that blockchains are a technology that, as such, is more facilitative of criminal activity than other technologies that have been used to such ends through history. Recent history furthermore illustrates that law enforcement agencies can successfully enforce the law in relation to criminal activity facilitated to blockchains, and that the latter's tamper-evidence even sometimes facilitates law enforcement agencies' task. As a matter of fact, DLT's tamper-resistant nature means that they can provide records of transactions that can be very useful for law enforcement purposes.

From this perspective, there does not appear to be any need for immediate policy action in this domain. Rather, the European Commission should adopt a wait-and-see approach and continue to monitor related developments and, if problems emerge, these could best be dealt with during the review of other relevant legislation (such as the AML Directive). This could be done in the context of the next bi-annual Supranational Risk Assessment Report to be released in 2021.[544]

5.2.4. Tension between blockchain reality and legal reality

In relation to the discrepancies that can exist between information as depicted on-chain and its counterpart in the analogue world (such as where a change of ownership that occurs off-chain but fails to be registered on the ledger) our research has shown that this is not an issue unique to blockchains, and not necessarily due to any particular features of the technology. Indeed, where appropriate design and governance decisions are adopted, blockchain reality and legal reality can be aligned. Thus, we would identify this as primarily a technical design and human governance issue. Indeed, the recent adoption of legislation in Liechtenstein that foresees a role for new intermediaries in coordinating off-chain and on-chain information can be seen as one possible solution to remedy possible discrepancies. Time and experience will reveal whether this is a successful approach, however, the idea itself underlines that discrepancies between on-chain and off-chain information can be addressed through appropriate solutions. Liechtenstein has chosen one of multiple different options to align on-chain and off-chain information and its approach will prove to be a valuable experiment which other jurisdictions can learn from. We recommend that the European Commission continue to monitor this and related developments through the adoption of a wait-and-see approach to evaluate whether, in the future, it may be necessary to adopt similar initiatives at EU level.

Should the European Commission already want to adopt a more proactive approach at this moment in time, it could again encourage the development of technical and governance solutions that are aimed at aligning on-chain and off-chain information. In order to encourage the adoption of suitable technical and governance solutions in relation to blockchain projects throughout the EU, the European Commission could adopt non-legislative measures that would draw attention to potential solutions among the wider industry, and help industry identify how blockchain design and governance could

[544] Also see 'Commission assesses risks and implementation shortcomings in fight against money laundering and terrorist financing: Questions and Answers' (July 2019), https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_4369. (last accessed on 24 January 2020).

be facilitative of legal compliance in line with what has already been outlined above. For example, the Commission could draft related guidance on best practices for aligning off-chain and on-chain information or encourage industry groups to draft related guidance, which assembles best practices that could so far be observed in relation to this issue. Initiating a broader discussion on how blockchains could be designed from both a technical but also a governance perspective in order to facilitate effective compliance with existing regulation would thus be of broader benefit. This could be done together with relevant stakeholders such as the Blockchain Observatory and Forum and INABTA (as the main blockchain industry association in the EU – at least at this stage) and other relevant actors (which might only emerge in the future).

Furthermore, the European Commission could support research efforts that experiment with different options in view of identifying best practices. Regarding timing, this is an effort that it should be able to conclude within 12-24 months. Indeed, this appears to be an important point as also in relation to the two preceding points we have found that the perceived regulatory issues in relation to blockchains appear to not so much be the consequence of regulatory shortcomings but rather of a lack of practical transposition of legal requirements that are in themselves clear[545]

5.3. Assessment of policy options for legal issues regarding smart contracts

5.3.1. Application of Contract Law

With regard to the question of the application of Contract Law, it has been observed that domestic contract law applies to smart contracts where these qualify as legal contracts. Whereas smart contracts by no means always qualify as legal contracts, they sometimes can where they meet the relevant definition of a valid contract in national legislation. Pursuant to our research findings, this is not seen as a cause for concern by relevant stakeholders. As a result, no specific issues that would require supranational action appear to emerge in this respect. As a consequence, our general policy recommendation is accordingly that no specific action needs to be taken at this stage: the European Commission should thus, first and foremost, adopt a wait-and-see approach and only take action if pertinent reasons emerge that would make supranational action a requirement in this context. In the context of its wait-and-see approach, the Commission should monitor ongoing efforts in other domains, such as at UNIDROIT.[546] Indeed, as an intergovernmental organisation tasked with the unification of private law, UNIDROIT's initiatives pursue a harmonising objective throughout EU Member States and beyond. Whereas UNIDROIT's initiative on smart contracts is still in its very early stages, its work is set to continue in 2020 and might generate important insights also from the perspective of the Digital Single Market and a potential need for related legal reform.[547]

As noted in Chapter 2, one specific aspect relating to the validity and enforcement of (smart) contracts is that of cross-border transactions, an element that is very important from a Digital Single Market perspective. Smart contracts are expected to be widely

[545] It is worth pointing out, however, that in some jurisdictions a different conclusion has been reached, such as in Liechtenstein which, as seen above, decided to revise elements of its civil law as a result of the emergence of blockchain technology.
[546] 'UNCITRAL/UNIDROIT, 'Workshop on smart contracts, artificial intelligence and distributed ledger technology – summary of conclusions published', https://www.unidroit.org/89-news-and-events/2663-uncitral-unidroit-workshop-on-smart-contracts-artificial-intelligence-and-distributed-ledger-technology-summary-of-conclusions-published (last accessed on 19 December 2019).
[547] 'UNCITRAL/UNIDROIT Workshop on smart contracts, artificial intelligence and distributed ledger technology – summary of conclusions published', https://www.unidroit.org/89-news-and-events/2663-uncitral-unidroit-workshop-on-smart-contracts-artificial-intelligence-and-distributed-ledger-technology-summary-of-conclusions-published (last accessed on 19 December 2019).

deployed in cross-border transactions, raising the question of whether a smart contract that is recognised in Member State A will also be recognised in Member State B. Our research has revealed that there can be scenarios where this is not necessarily the case, such as where jurisdiction A does not require that that particular contract be in writing but jurisdiction B does require semantic written contracts for that particular kind of contract. This, of course is not an issue which is specific to smart contracts but one which can also be observed in relation to any kind of contractual transaction in general and electronic contracts specifically.[548] Even though diverging national requirements on contract validity can be an obstacle from a Digital Single Market perspective, their persistence throughout time also seems to be evidence of the fact that these divergences pursue important public policy objectives. What is more, our research has shown that existing secondary legislation, most notably the Rome I regime as well as additional instruments in private international law seem well-equipped to deal with such divergences in contract law in that they enable parties to choose applicable law. Our analysis above has, however, also revealed that there may be uncertainty as to whether Article 3(1) of the Rome I Regulation applies to blockchain-based assets such as utility tokens. Whereas we have concluded above that it cannot necessarily be taken for granted that it does, this matter is not settled and may hence create a lack of legal certainty for those wishing to deploy smart contracts in pan-European settings. Whereas this is a matter that would ultimately have to be clarified by the Court of Justice of the European Union or a revision of the Rome I Regulation, these are both solutions that take a long time to come about. Should the European Commission strive to adopt a more proactive approach in this respect immediately, it could issue regulatory guidance regarding its own interpretation of this legal matter. Whereas this could still be overturned by a subsequent judgment, it might not be, and might bring about legal certainty more quickly, as indeed this is something that could probably be achieved within a couple of months. Alternatively, this is a matter that could be put on the table on the occasion of the next revision of the Rome I regime.

5.3.2. The need for written form of the contract

It appears that there is no need for immediate regulatory action concerning the need for written form of the contract as it exists in the national contract law regimes of different Member States. It is true that our review of national legislation has shown that there can sometimes be requirements in national legislation for written contracts to exist alongside the smart contract computer code, and these requirements may impede the development of some smart contract use-cases. However, we have also seen that national requirements regarding the form of the contract seem to operate in a technology-neutral manner to protect important policy objectives. What is more, in many scenarios these requirements can be fulfilled where the contract is in electronic form. There is no indication that these requirements, which fulfil such policy objectives, could not be implemented in relation to DLT through adequate design solutions that allow for a linking of the digital contract and the paper counterpart.

We thus consider that there is no need for a specific policy to be initiated in this respect at this moment in time. Rather, the Commission should wait-and-see whether existing national requirements on certain contracts being written in prose turn out to be an unjustified impediment to the developments of smart contracts in the EU and, should this be so, consider policy options to change this.

5.3.3. Smart contracts and Consumer Law

Our analysis has revealed that whereas automated enforcement through smart contracts may present advantages to consumers, such as an automated enforcement of their right in case of flight or train delays, there are also considerable concerns in this

[548] Due to the general nature of this legal issue, it was not included as part of the policy matrix.

respect. Indeed, many of the stakeholders we interviewed identified consumer protection as a key policy priority. At the same time, consumer law is a technology-neutral framework, which applies to smart contracts as well. We conclude from this that the dangers to consumer protection are not apparently the result of inadequacies in consumer protection law but rather due to an insufficient awareness and enforcement of related rules. In general, the European Commission should first and foremost adopt a wait-and-see approach, determining whether, over time, precise issues arise when it comes to the application of consumer law to blockchains. Indeed, whereas most stakeholders agree that this is an important issue, our analysis has also shown that no concrete examples of possible shortcomings in the law or a lack of technological neutrality in its application could be identified.

Regarding the specific issue of the right to withdrawal under the Consumer Rights Directive, a more proactive approach by the European Commission could, however, be of much benefit.[549] Indeed, we recommend that on the occasion of the next revision of this legal regime (in accordance with Recital 62 of the Consumer Rights Directive), the Commission considers whether consumers' withdrawal rights create an undue burden in respect of smart contracts.[550] In the interim, the European Commission could also choose to adopt regulatory guidance on how precisely consumer protection law applies to smart contracts. Specifically, Article 9 EU Directive 2011/83/EU on consumer rights foresees that consumers have a right of withdrawal from consumer contracts concluded at a distance or off-premises without giving a reason, for 14 days. If the trader has not provided the consumer with the information on the right of withdrawal as required, the withdrawal period shall expire 12 months from the end of the initial withdrawal period.[551] If the trader has provided the consumer with the information on the withdrawal right within 12 months from the day of the conclusion of the contract (in case of provision of services contracts) or coming into possession of goods, the withdrawal period shall expire 14 days after the day on which the consumer receives that information. Article 16 of Directive 2011/83/EU also provides for exceptions from the right to withdrawal and the right to withdrawal does not apply in relation to 'service contracts after the service has been fully performed if the performance has begun with the consumer's prior express consent, and with the acknowledgement that he will lose his right of withdrawal once the contract has been fully performed by the trader'. In those cases where there is a service contract and the consumer expressly consents to a restriction to her right of withdrawal, the right to withdrawal no longer applies once the service has been fully performed. Our analysis above has revealed that this may apply in some circumstances where smart contracts are used and clarification as to when this is the case and what related implications are would provide more legal certainty to those using smart contracts.

A further specific consumer law question where regulatory guidance adopted by the European Commission would be helpful is that of Article 3(2)(l) of the Consumer Rights Directive, which excludes from its application contracts 'concluded by means of automatic vending machines or automated commercial premises'. Our analysis has revealed that there is an argument to be made that this exemption also applies to smart contracts. The Commission could update its existing guidance document on the Consumer Rights Directive to clarify whether it considers smart contracts to be caught by this exemption, and if so under which circumstances. This exercise could also be done immediately or on the occasion of the first review of the 'New Deal for Consumers'

[549] See analysis in Section 3.3.1.3 above.
[550] See analysis in Section 3.3.1.3 above.
[551] Article 10, 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 Text with EEA relevance, *OJ L 304,* 22 November 2011, p.78.

package in 2024.[552] The issuing of regulatory guidance on these specific points should be possible in a timeframe of 12-24 months. Additionally, the enforcement of related norms by consumers, consumer rights organisations, and public authorities would be a powerful means of ensuring that consumer protection is indeed applied in practice.

It follows that the suggested policy response here is a mixture of wait-and-see and regulatory guidance. Considering that this is a space that is still in full development, the Commission should continue to monitor related developments and assess in a few years whether smart contracts have generated consumer protection concerns that could not be addressed through existing consumer law. On the other hand, regulatory guidance, which could be adopted within 12-24 months, on these issues would contribute towards more awareness regarding applicable norms amongst stakeholders. Collaborative efforts with relevant stakeholders could moreover lead to a more compliance in practice and also the development of original technical approaches towards achieving these aims.

5.3.4. Smart Contracts and pseudonymity

Blockchains are typically characterised by their pseudonymous nature as network participants, which can be natural or legal persons or machines, are usually identified through a pseudonymous identifier. However, it has been observed above that in some circumstances, national contract law requires an identification of the parties to a contract. This is not necessarily impossible to achieve where blockchains are used, it generally just requires the usage of additional processes deployed to ensure that the parties to a smart contract are in fact known. Notwithstanding this, our research has shown that there appears a lot of uncertainty as to how this could best be achieved.

The European Commission could help clarify these issues relating to smart contracts and pseudonymity, for instance by encouraging industry organisations such as INABTA in addition to service providers in this domain to elaborate standard contractual clauses related to identification which could be used by actors wishing to use blockchains. This would make it easier and less costly for companies using this technology to achieve legal compliance and also make it easier for aggrieved parties to obtain redress as they could more easily discover the identity of their counterparty. This could be done in a period of 1-2 years. Beyond this, the Commission should also monitor, and if considered appropriate, encourage the development of digital and/or SSI systems, such as for instance through research funding. This could be done relatively quickly, such as when the next calls for various EU funding schemes are issued.

5.3.5. Smart contracts and jurisdiction

Regarding jurisdictional questions around blockchains, it has been amply stressed that oftentimes, it is difficult to determine which law applies where blockchain networks span many different jurisdictions. Indeed, the network operators and nodes can be located in different locations (so that different legal systems may apply to them) and equally, the participants in the network such as the contracting parties are also not necessarily based in the same jurisdiction. However, existing supranational legislation such as the Brussels I and Rome I regimes appear well-suited to govern related issues, which indeed do not appear to be specific to blockchains but rather apply to transnational (technical) networks in general. Hence, existing legal mechanisms already provide tools enabling parties to a blockchain-based smart contract to deal with uncertainties regarding jurisdiction.

At this stage, there appear to be no indications that these legal regimes are failing to be technology-neutral or that they disadvantage smart contracts, and thus that the

[552] See Article 6 of the Directive on the better enforcement and modernisation of Union consumer protection rules.

Commission should take action. However, the Commission is encouraged to continue monitoring the area of smart contracts and jurisdiction and close attention should be paid to smart contracts on the occasion of the next revision of the Rome I and Brussels I regimes.

5.3.6. Capacity to contract and the protection of minors

Questions around the identity of the participants to a smart contract have also emerged regarding the capacity to contract and the protection of minors. Whereas there does not appear to be an immediate need for regulatory intervention in the domain, the European Commission could support initiatives that seek to provide innovative solutions in this domain (such as through research funding). This could be done relatively quickly, such as when the next calls for various EU funding schemes are issued. This could apply in particular to governance solutions that enable identification in a privacy-preserving manner as well as more innovative forms of digital and/or SSI.

5.3.7. Opacity

Our analysis has revealed that it is sometimes considered that due to their technical complexity blockchain-based use cases can be hard to fashion in a transparent manner. For instance, smart contract code is only accessible to those that understand coding language and as a result, most parties are unable to verify whether what is conveyed to them in prose actually corresponds to these tools' technical set-up. This, of course, is in no way an issue that is unique to blockchains. Rather, it applies to any technical system using computer language instead of prose.

It has, however, been observed above that Article 10 of the E-Commerce Directive addresses this in B2C relations to the extent that it requires the consumer to be provided with clear, comprehensible and unambiguous information prior to deploying the contract.[553] It provides that consumers ought to receive information regarding, inter alia, the technical steps to conclude a contract, the technical means to identify and correct input errors and the languages offered for the conclusion of the contract (except where the contract is concluded exclusively through electronic mail).[554] Services providers also ought to indicate relevant codes of conduct to which they subscribe and information as to how they can be consulted electronically (except where the contract is concluded exclusively through electronic mail).[555] Contractual terms and conditions ought to be made available in a manner that allows for storage and reproduction.[556] Article 6 of the Consumer Rights Directive provides that consumers benefit from information rights in distance and off-premise contracts, which includes, inter alia, information about the main characteristics of goods or services, the trader's identity and her geographical address as well as contact details, information regarding price and other costs etc.[557] Thus, the law already has an existing remedy to the opacity issue in B2C relations, where remedying opacity is particularly important.

As a result, there does not appear to be an immediate need for regulatory intervention with regard to opacity, given the existence of an established transparency regime under Article 10 of the E-Commerce Directive. It is, however, subject to debate whether this regime provides sufficient guarantees in relation to electronic contracts in general and smart contracts. This indeed appears to be a topic of general importance in the Digital Single Market. We have indeed moved away from a time where most contracts were concluded orally or in writing to one where electronic contracts or implementations of contracts govern ever more scenarios of everyday life and business transactions. Some

[553] Article 10(1) of the E-Commerce Directive.
[554] Article 10(1) of the E-Commerce Directive.
[555] Article 10(2) of the E-Commerce Directive.
[556] Article 10(3) of the E-Commerce Directive.
[557] Article 6 of the Consumer Rights Directive.

have expressed concerns as to what this means for understandability and power relations between individuals, the private sector and the state in general.[558] General efforts at making electronic contracts of all forms more transparent and user-friendly thus seem a worthwhile exercise. There are a number of ways in which this could be achieved, such as by creating interfaces that enable for the translation of computer code into prose. Given the importance of this issue, the Commission could encourage related research funding. This could be done relatively quickly, such as when the next calls for various EU funding schemes are issued. Related efforts would benefit the blockchain domain but also others beyond.

5.3.8. Smart Contract Arbitration Mechanisms

There appear to be no principled legal hurdles to using smart contract arbitration mechanisms under the current state of the law and to relying on such regimes in domestic legislation.[559] However, smart contract arbitration mechanisms need to comply with the general legal requirements applicable to arbitration proceedings, which sometimes require the filing of certain documents in state courts. That being the case, such DLT-based mechanisms cannot be purely digital but require the fulfilment of some analogue requirements. At present, it is too early to determine whether these requirements merely seek to achieve public policy objectives in a technology-neutral manner or whether they might unduly limit the development of smart contract arbitration mechanisms in the EU.

The European Commission could, however, consider the adoption of standard arbitration clauses to help businesses relying on such processes ensure legal compliance and secure consumer protection. This would enable smaller businesses without in-house legal counsel to make sure that their smart contract arbitration mechanisms comply with relevant legislation. Given that relevant legislation is often national legislation, this may, however, be a task that can more suitably be executed by national authorities. This could be done in a collaborative effort together with relevant stakeholders at national and supranational levels, such as the EU Blockchain Forum and Observatory or INABTA, national blockchain associations as well as national and European consumer protection associations. The timeframe for this exercise should be in the range of one to three calendar years. These clauses could then be used by businesses, including SMEs that may lack capacities to fashion these independently, in order to ensure that existing legal requirements are being met in relation to smart contract arbitration. Whereas such an initiative may facilitate matters for smaller businesses, public authorities pondering the adoption of such measures should also consider that this may be a time- and labour-intensive exercise, considering that these clauses would need to be regularly updated.

It has also been observed that requirements regarding the involvement of Member State courts in arbitration proceedings risks making these tools less attractive. It is too early to determine whether these requirements continue to serve important public policy objectives that ought to apply in a technology-neutral manner or whether, to the contrary, they risk disincentivising innovative processes that would ultimately ensure higher judicial protection as consumers might be more likely to rely on such arbitration mechanisms than state courts, mainly for reasons of time and cost. The Commission should continue to observe related developments to determine whether ultimately, policy interventions may become necessary in this area.

---

[558] Luca Belli and Nicolo Zingales, Platform Regulations, 'How Platforms regulated and how they regulate us' (December 2017), https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/19402/Platform%20regulations%20-%20how%20platforms%20are%20regulated%20and%20how%20they%20regulate%20us3.pdf?sequence=4&isAllowed=y (last accessed on 24 January 2020).

[559] On smart contract arbitration mechanisms, also see Section 3.3.1.8 and following of this report.

5.3.9. Notarisation

In respect of notarisation requirements in domestic legislation, our research has revealed that, on the one hand, blockchains might be a useful tool for notaries to carry out their professional obligations in a more speedy and efficient manner, and blockchain may be a useful tool for existing notarisation requirements. At the same time, it has however also been seen that existing legal notarisation requirements that require the involvement of notaries may make it difficult for certain processes, such as the creation of new business entities, to occur solely in the digital realm.

We recommend that the European Commission continues to monitor these developments in order to determine whether existing rules are pertinent for the protection of given public policy objectives and apply in a technology-neutral manner or whether it may be necessary to revise these rules in case they unduly stifle the development of blockchain-based business models. There is already secondary legislation in place that seeks it make it easier to found companies digitally, notably the Directive on the Use of Digital Tools in Company Law, which obliges Member States to (with some limitations) facilitate the online formation of companies. The next revision of this legislative regime in 2024 would provide a suitable opportunity for the Commission to evaluate whether this regime ought to go further, such as because it proves to create undue burdens on the use of blockchain technology.[560]

5.4. Assessment of policy options for legal issues regarding utility tokens

5.4.1. The lack of legal certainty and regulatory fragmentation

Our analysis on utility tokens has shown that there is currently large agreement that the use of so-called utility tokens is burdened by a lack of legal certainty and regulatory fragmentation.[561] The existing degree of regulatory fragmentation is in the future likely to be increased by the fact that a number of jurisdictions, including EU Member States, are pondering the adoption of national legislation on utility tokens. As a result, some have called for harmonised EU legislation on this matter. It is, however, also important to note that there is no consensus on the need for such legislation. Indeed, some have stressed that they have never encountered legal obstacles in relation to utility token projects.[562] Others are sceptical whether it would really be possible to have bespoke legislation on utility tokens considering that many tokens are hybrids and difficult to catch by a single category.

European regulators could thus consider two policy options in order to avert the pejorative effects of lacking legal certainty and regulatory fragmentation in the Digital Single Market. Firstly, they could reduce such uncertainty and fragmentation through the issuing of regulatory guidance as to how related legal frameworks apply to utility tokens. Indeed, whereas there currently is no bespoke regime applying to such tokens, setting out aspects such as when financial regulation applies, or what obligations derive from other aspects of supranational law such as consumer protection law could likely remove some of the uncertainties in this domain. A second option is to consider the creation of a supranational regime on utility tokens that would create detailed legal requirements applying to this category of tokens (in addition to those legal requirements which apply to them anyways). Both options offer advantages and disadvantages that would need to be carefully considered.

[560] See Article 3 of Directive 2019/1151.
[561] Please refer to Section 3.3.2 above. See also interview with Gide Loyrette Nouel.
[562] Interview with The Marshall Plan Holding.

The first option consists in the issuing of regulatory guidance as to how existing legal frameworks apply to utility tokens, such as for instance supranational consumer protection instruments. However, it has been seen that utility tokens are caught by both national and European legislation. Whereas the Commission could only initiate guidance on the latter, the effect would be limited as this policy option would be unable to address concerns that have arisen in relation to national law. What is more, the issuing of regulatory guidance at EU level would be unable to address concerns related to the growing regulatory fragmentation as different domestic regimes would still be in place. Moreover, the European Court of Justice could in the future disagree with a given interpretation adopted by the Commission with the result that there would have been only an illusion of legal certainty. This would be the quickest of the two policy options considered here as such guidance could probably be issued in a timeframe of 12-24 months.

The adoption of EU secondary legislation could also help solve the difficulties associated with fragmentation and lacking legal certainty, both of which risk being detrimental to the Digital Single Market project. An EU framework on utility tokens would have the benefit of creating a harmonised legal framework that would apply throughout the European Union, resulting in cost reductions for those that wish to offer pan-European services involving utility tokens. At the same time, it may attract businesses that use utility tokens to the European Union and hence strengthen the Digital Single Market and its global competitiveness. As regards timing, the initiation of secondary legislation should take between three and four years.

At the same time, it is paramount that this legislation be designed in a manner that is technology-neutral and can account for the fact that many tokens are hybrid tokens that fail to neatly fall within a specific category. Indeed, it has been seen above that there are dangers associated with the adoption of a European directive or regulation on utility tokens at this stage. On the one hand, many doubt whether it is practically possible to adopt a legal definition of a utility token based on functional criteria as what is qualified as a 'utility token' often also assumes characteristics of means of payment or securities. If this is the case, the adoption of a separate legal category of the utility token may aggravate rather than reduce regulatory uncertainty and fragmentation. Where a token is of a hybrid nature there then is a challenge to either qualify that token in terms of its prevailing characteristic or to say that as soon as it has some financial elements, it is included in the scope of financial regulation.[563] Others have, however, noted that the category of the utility token could also be a catch-all category (catching all tokens not caught by financial regulation or another *lex specialis*).[564] Such as solution appears to have been adopted in Malta as the Virtual Financial Assets Act Bill distinguishes various categories of digital assets, including virtual token, which falls outside the scope of financial regulation. It is defined as a form of digital medium recordation whose utility, value or application is restricted solely to the acquisition of goods or services, either solely within the DLT platform on or in relation to which it was issued or within a limited network of DLT platforms'.[565]

It is worth stressing that some have also expressed concerns that business models relying on utility tokens are really prone to replace existing models such as payment, subscription or financing through advertisements. However, the analysis in Section 3.3.2 has revealed that it cannot be taken for granted that this is indeed the future of utility tokens as some consider that they may play a more marginal role in the future

[563] Based on feedback received during the workshop (more information on the workshop can be found in the introduction of this report).
[564] Based on feedback received during the workshop (more information on the workshop can be found in the introduction of this report).
[565] Article 1(2)(2) of the Malta Virtual Financial Assets Act Bill.

than is often assumed. If the European Union were to consider the adoption of a bespoke legal framework on utility tokens, this is something that ought to be carefully considered as there are considerable downsides to the adoption of legislation that has limited practical value. Furthermore, it has been stressed that it may simply be too early for the EU to regulate at the current stage where use cases, risk of harms and definitions remain unclear.[566]

Where regulation is chosen as the preferred policy option, it appears that traditional secondary legislation, maybe designed through a co-regulatory effort, is the most promising avenue. Indeed, self-regulation appears undesirable as it is not clear that the private sector would have the required incentives to create a regime protective of consumer interests. What is more, the key concerns that have been identified are the lack of legal certainty and regulatory fragmentation, which are best addressed through formal EU legislation that is publicised according to legal requirements and takes precedence over national norms in line with the principle of the supremacy of EU law. It is worth noting that many stakeholders have stressed that where secondary legislation is adopted, a regulation would be preferable to a directive as the latter may not necessarily add further legal certainty to this area.[567]

5.4.2. Consumer protection (including prospectus requirements)

Many stakeholders have stressed the importance of ensuring effective consumer protection in relation to utility tokens. Indeed, our stakeholder consultations have revealed that although consumer protection law applies to utility tokens, there often appears a lack of awareness that this is the case, and different implementations in different Member States have led to fragmentation in the internal market. In order to tackle perceived gaps, some are suggesting that the creation of a bespoke prospectus requirement for utility tokens would be a solution.

Whereas some have called for an extension of the prospectus regime to utility tokens – which would correspond to the adoption of new secondary legislation – it is also important to highlight that there may be disadvantages associated with that solution. First, a regime designed for securities would be extended to commodities, without it being apparent that both asset classes require the same regime. Second, the application of the prospectus regime would impose considerable compliance costs on blockchain projects, some of which may not be proportionate to the task to be achieved. The exercise would also take time – we are estimating that it would take between 3 and 4 years. As such, an alternative form of transparency requirements may prove more suitable. A first step could be the adoption of standards by industry that are subsequently endorsed by regulation. The European Commission could take on a steering role in initiating such industry efforts. This could result in the provision of more detailed information to consumers as well as a right to seek remedies in court in cases where industry fails to comply with the transparency obligation. This could arguably be done more quickly. We are estimating that the relevant timeframe here would be around two calendar years. It is moreover worth noting that it would be important to determine how related obligations would relate to existing information requirements in EU consumer law and whether the latter does not already address the consumer protection concerns that have been noted.

As it is not evident that existing EU secondary legislation is per se insufficient to address the consumer protection concerns that have arisen, it appears that the most suitable policy option in this respect would be guidance by the European Commission and/or

[566] Based on feedback received during the workshop (more information on the workshop can be found in the introduction of this report).
[567] Based on feedback received during the workshop (more information on the workshop can be found in the introduction of this report).

national authorities regarding how precisely consumer protection law applies to utility tokens. Indeed, our research has revealed that whereas stakeholders concur that consumer protection is a pivotal concern in relation to utility tokens, no concrete examples of shortcomings could be identified. Moreover, some have warned that adding additional consumer protection requirements may render this framework too complex and detailed.[568] This could take the form of an independent exercise or be done in coordination with relevant stakeholder groups such as INABTA and/or the European Blockchain Observatory and Forum. It should take between 12-24 months to complete this exercise. Beyond, the enforcement of related norms by consumers, consumer rights organisations, and public authorities would be a powerful means of ensuring that consumer protection is indeed applied in practice. In addition, the adoption of industry standards subsequently endorsed through legislation could provide more transparency for consumers. It follows that the suggested policy response here is a mixture of wait-and-see as well as regulatory guidance.

Considering that this is a space that is still in full development, the Commission should continue to monitor related developments and assess in a few years whether utility tokens have generated consumer protection concerns that could not be addressed through existing consumer law. For the time being, regulatory guidance on these issues would contribute towards more awareness regarding applicable norms amongst stakeholders. Collaborative efforts with relevant stakeholders could moreover lead to a more compliance in practice and also the development of original technical approaches towards achieving these aims. In case this fails to provide satisfactory results, secondary legislation should be considered.

5.4.3. Trading on secondary markets

Our research has identified that many stakeholders have highlighted that there is a lack of legal clarity concerning the trading of utility tokens on secondary markets[569] Also in this context, the issuing of regulatory guidance by the European Commission could help achieve more clarity; regulatory guidance on the rules applicable where utility tokens are traded on secondary markets would be important to clarify related rights and obligations and improve legal certainty in the Digital Single Market.

It is true that some stakeholders have flagged the lack of transparency and investor protection that may exist in relation to unregulated trading platforms (e.g. those trading platforms that are not trading tokenised financial instruments). In order to remedy the lack of transparency and investor protection, rules on governance arrangements and conflicts of interests can be necessary in line with what has already been noted in relation to other areas above. At the same time, there have been no indications in the literature or from stakeholders that the case for new supranational legislation can be made. Considering the widespread perception by stakeholders that trading on secondary markets is a domain where many regulatory problems arise, a passive wait-and-see approach by the Commission might seem insufficient to assure stakeholders. As such, a suitable policy option appears to be that of the Commission encouraging the adoption of standards by industry that are subsequently endorsed by regulation if need be. The timeframe of this exercise should be in the range of around two calendar years (and more if the subsequent adoption of regulation proves necessary). This could result in the provision of more detailed information to consumers as well as a right to seek remedies in court in cases where industry fails to comply with the transparency obligation. In case this fails to provide satisfactory results, secondary legislation (which

[568] Based on feedback received during the workshop (more information on the workshop can be found in the introduction of this report).
[569] Interview with Gide Loyrette Nouel.

may or may not be inspired by the standards that have been developed) should be considered.

5.5. Conclusion

This section has examined what policy options might be most suitable in light of the general legal issues, legal issues in relation to smart contracts, and legal issues in relation to utility tokens that were identified in previous chapters. A brief overview was provided in relation to each legal issue before various possible policy options were introduced and discussed.

We have identified the following policy options in relation to each legal issue that was identified.

Firstly, with regard to the general legal issues that have emerged regarding blockchain technology, we have examined the challenges of allocating responsibility in decentralised systems, specifically in relation to *responsibility for legal compliance and liability*. These challenges are not due to shortcomings of the respective legal frameworks but rather to the fact that blockchain systems and specific use cases thereof may not have been designed with a view to complying with legal requirements. As a result, we consider that (i) no specific policy response is needed and recommend that the European Commission adopt a wait-and-see approach. Furthermore, (ii) better technical design could enhance compliance. Whereas this is not foremost a task for public authorities, the Commission could incentivise industry efforts to this effect should it want to. Lastly, (iii) stricter law enforcement by relevant national and supranational agencies would underline that compliance is not optional and create incentives for compliance for industry.

Next, we have examined *potential barriers in sectoral legislation* and found that Anti-Money Laundering law is of particular concern to stakeholders. Our research has shown that ensuring compliance with AML legislation is essentially a governance question (for the actor using blockchain) as well as a question of the effective enforcement of existing regulations (from the public authority perspective) and thus does not require a specific policy response. Possible policy options are therefore that (i) the Commission adopt a wait-and-see approach. Should the Commission wish to adopt a more active approach, it could (ii) proactively encourage that blockchain-based AML systems are designed in order to ensure compliance with existing regulation from a technical perspective such as through research funding. Additionally, (iii) the adoption of standards terms and conditions or contracts could be used to coordinate compliance (e.g. model contracts ensuring that the related sharing of information between numerous actors for AML purposes is respected).

A common concern has also been that of the *protection of fundamental legal principles and mandatory rules*. Our research revealed that existing principles appear well-suited to addressing problems associated with the criminal use of this technology. There is thus no immediate need for a concrete policy action and (i) the European Commission should adopt a wait-and-see approach.

Regarding the *tension between blockchain reality and legal reality*, we have identified this as a technical design and human governance issue not unique to blockchains. Our research has revealed no immediate need for policy action, and we recommend (i) the adoption of a wait-and-see approach in this context. Should the European Commission already want to adopt a more proactive approach, it could (ii) encourage the development of technical and governance solutions that are aimed at aligning on-chain and off-chain information (such as guidance on best practices) and (iii) provide research

funding for projects seeking to address such issues (which are also of broader relevance for the digital economy).

The chapter then turned to examine smart contracts. Firstly, we examined the *application of contract law* to smart contracts. Whereas smart contracts by no means always qualify as legal contracts, they can in cases where they meet the relevant definition of a valid contract in national legislation. Pursuant to our research findings, this is not seen as a cause for concern by relevant stakeholders. As a result, (i) no specific action needs to be taken at this stage, and the European Commission could adopt a wait-and-see approach. Regarding the specific case of cross-border transactions, it may be that a contract valid in one jurisdiction is not valid in another. Usually, this would be governed by the Rome I Regulation. However, in this specific case, uncertainty surrounds the question of whether Article 3(1) of the Rome I Regulation applies to blockchain-based assets such as utility tokens. Whereas this is a matter that would ultimately have to be clarified by the Court of Justice of the European Union or a revision of the Rome I Regulation, the Commission could (ii) issue regulatory guidance on this matter.

Secondly, we examined the fact that some *national contract law provisions require a written contract* in some circumstances. Our research revealed that such requirements seem to operate in a technology-neutral manner to protect important policy objectives. What is more, in many scenarios these requirements can be fulfilled where the contract is in electronic form. We thus recommend that (i) the Commission adopt a wait-and-see approach.

Thirdly, we examined the *application of consumer law to smart contracts*. As stakeholders could not identify specific legal issues arising in this respect, the Commission could (i) adopt a wait-and-see approach. Regarding the specific issue of the right to withdrawal under the Consumer Rights Directive, the Commission could (ii) engage a discussion on whether consumers' withdrawal rights create an undue burden on smart contracts as part of the next revision of this legal regime (in accordance with Recital 62 of the Consumer Rights Directive). In the interim, it could (iii) also choose to adopt regulatory guidance on how precisely consumer protection law applies to smart contracts, particularly in relation to Article 9 EU Directive 2011/83/EU (the right of withdrawal) and Article 3(2)(l) of the Consumer Rights Directive (on contracts 'concluded by means of automatic vending machines or automated commercial premises').

Regarding *smart contracts and pseudonymity*, the Commission could (i) encourage the adoption of standard contractual clauses related to the identification of parties that could be used by actors wishing to use blockchains. Beyond this, the Commission (ii) could also monitor this issue, and if considered appropriate, encourage the development of digital and/or SSI systems, such as for instance through research funding.

Concerning *smart contracts and jurisdiction*, existing supranational legislation such as the Brussels I and Rome I regimes appear well-suited to govern related issues so that (i) the adoption of a wait-and-see approach seems well-suited in this domain.

With regard to the *capacity to contract and minors*, there does not appear to be an immediate need for regulatory intervention in the domain, favouring a (i) wait-and-see approach. The Commission could, however, (ii) provide research funding for projects seeking to provide innovative solutions.

In relation to *opacity*, existing supranational secondary legislation already seems to contain mechanisms to address the disadvantages that opacity may generate for

consumers, in particular Article 10 of the E-Commerce Directive and Article 6 of the Consumer Rights Directive. As a result, there does not appear to be an immediate need for regulatory intervention with regard to opacity. Rather, the Commission could adopt a (i) wait-and-see approach. Notwithstanding this, the question of how to make electronic contracts in general and smart contracts specifically easier to understand is one of general importance in the Digital Single Market. As such, the Commission could also (ii) encourage related research funding for projects seeking to achieve this objective.

Then, for *smart contract arbitration mechanisms*, we have concluded that it is at present too early to determine whether requirements to file documents in national courts merely seek to achieve public policy objectives in a technology-neutral manner or whether they might unduly limit the development of smart contract arbitration mechanisms in the EU. A (i) wait-and-see approach could thus provide further clarity in this respect. The Commission could, however, also (ii) encourage the adoption of standard arbitration clauses to assist and help businesses in this regard.

Lastly, in relation to smart contracts and *notarisation*, we recommend that the European Commission (i) continues to monitor developments in order to determine whether existing rules are pertinent for the protection of given public policy objectives and apply in a technology-neutral manner, or whether it may be necessary to revise these rules.

After having examined various legal issues related to smart contracts our analysis turned to utility tokens. Firstly, we considered the concern identified by stakeholders regarding the *lack of legal certainty and regulatory fragmentation*. Our analysis found that European regulators could consider two policy options: (i) they could reduce uncertainty and fragmentation through the issuing of regulatory guidance as to how related legal frameworks apply to utility tokens or (ii) consider the creation of a supranational regime on utility tokens.

Secondly, we focused on the application of *consumer protection rules* (including prospectus requirements) to utility tokens. Our research showed that although consumer protection law applies to utility tokens, there often appears to be a lack of awareness that this is the case, and different forms of implementation in Member States have led to fragmentation in the internal market. In this respect, the Commission could (i) encourage the adoption of standards by industry which may subsequently be endorsed by regulation. Moreover, the (ii) adoption of guidance by the European Commission and/or national authorities regarding how precisely consumer protection law applies to utility tokens would appear to be a useful step.

Thirdly, regarding the *trading of utility tokens on secondary markets*, many stakeholders have highlighted that there is a lack of legal clarity concerning the trading of utility tokens on secondary markets. To address this matter, the Commission could (i) adopt regulatory guidance on the rules applicable where utility tokens are traded on secondary markets and (ii) encourage the adoption of standards by industry that are subsequently endorsed by regulation if need be. The below policy matrix summarises our findings.

Table 3 - Policy matrix

	Wait-and-See	Regulatory Guidance	Secondary Legislation	Other (e.g. **research funding**, opt-in regime, regulatory sandboxes, monitoring, best practices, standard terms and conditions or model contracts)
Legal issues regarding blockchain technology in general				
Responsibility for legal compliance and liability	X			
Potential barriers in sectoral (e.g. AML) legislation	X			X
The protection of fundamental legal principles and mandatory rules	X			X
Tension between blockchain reality and legal reality	X	X		X
Legal issues regarding smart contracts				
Application of Contract Law	X			X
The need for written form of the contract	X			
Smart contracts and Consumer Law	X	X		X
Smart contracts and pseudonymity				X
Smart contracts and jurisdiction	X			X

Capacity to contract and the protection of minors	X			X
Opacity	X			X
Smart Contract Arbitration Mechanisms				X
Notarisation	X			X
Legal issues regarding utility tokens				
The lack of legal certainty and regulatory fragmentation		X	X	
Consumer protection (including prospectus requirements)	X	X		X
Trading on secondary markets		X		X

The economic and social impacts that blockchain might support and the potential impacts of the policy options that might be adopted will be discussed in Chapter 5.

6. Chapter 5 – Analysis of the impact of blockchain technology on the economy and society

6.1. Introduction

Blockchain and distributed ledger technologies are increasingly in the news, most frequently as the underlying technology enabling a move from digitisation dominated by platforms and concentrated silos of data to a digitalisation based on decentralised technologies. The European Commission asserts that this holds great promise for the European economy and society.[570] However, at the same time, this is both a challenge and opportunity for policymakers and the development of legal frameworks at the regional, national, EU and international levels.

In the autumn of 2018, the European Parliament adopted two resolutions concerning distributed ledger technologies and blockchains, which highlighted the potential impacts of blockchain technology and called for a review of interoperability between blockchain systems; an in-depth investigation of legal implications, potential impacts on EU trade policy, potential social impacts and the development of guidelines for utility tokens. An important objective was to support European industry in developing the technology and ensuring a level playing field for global competition.

This Study is one of several commissioned to investigate these areas. This report provides a brief overview of the capabilities offered by blockchain technologies and the impact of the adoption of blockchain on the economy, socially and environmentally. Three particular areas of attention have been identified for this Study; broad blockchain trends, smart contracts and utility tokens.

It is expected that blockchains can make a new automated and distributed internet infrastructure possible, concurrently strengthening a shared economy and enabling the development of business model innovations. Blockchain is a technology that promotes user trust and makes it possible to share online information, agree on and record transactions in a verifiable, secure and permanent way. Blockchain can play a critical role in overcoming market failures by reducing information asymmetries between different market actors. It can provide market players with the needed mutual trust, and thus enable transactions that would have not taken place otherwise. Therefore, it is expected that blockchain will contribute to economic growth and foster local social development.

Blockchain is often mentioned alongside other recent technological innovations such as broadband, 5G, cloud computing, IoT, AI and big data analytics.

All these technologies, including blockchain, have created disintermediation. For example, mobile phones created disintermediation amongst fixed line providers and the recent advent of mobile wallets is creating disintermediation in the financial sector. Cloud services cause disintermediation by creating, managing and delivering digital service over the top[571] and artificial intelligence-powered processes to underwrite risk and extend credit instantly are creating disintermediation in the financial sector.

[570] European Commission. 2019. Tender Specifications for this Study on Blockchains: Legal governance and interoperability aspects. SMART 2018/0038.

[571] McKnight L. 2014. Over the virtual top: Digital service value chain disintermediation. 42nd TPRC Research Conference on Communication, Information and Internet Policy George Mason University School of Law, Arlington, VA September 12th 2014. https://www.researchgate.net/publication/265599051_Over_the_Virtual_Top_Digital_Service_Value_Chain_Disintermediation_Implications_for_Hybrid_Hetnet_Regulation (last accessed 22 January 2020).

Blockchain obviously has the capability to make a substantial change in the financial sector and many other areas. For example blockchain will create changes to financial intermediation structures[572] through the provision of direct links between lenders and borrowers, investors and investment opportunities.

We assert that while all the technologies have created disintermediation, blockchain is different to most of these technologies. The preceding technologies are generally purchased by a citizen, business or other entity and used by them for social or economic advantage. In the case of broadband and 5G, there are even national and pan-European[573] regulators to ensure communications markets work for everyone. Purchase of these technologies normally requires the consumer to check the quality and suitability of goods or services before a purchase is made (caveat emptor).

Blockchain creates a platform or marketplace through which numerous stakeholders communicate and transact. A platform used by many different stakeholders requires the establishment of the right conditions, to ensure the development of an open, secure, trustworthy, transparent, and EU law compliant data and transactional environment. This is therefore a primary focus for this Study. This chapter considers the economic and social impacts that blockchain might support and the potential impacts of policy options that might be adopted. This chapter achieves this broad objective by:

1. Considering the underlying characteristics of blockchain opportunities and the catalysts and drivers to achieve socio-economic impacts;
2. Investigating barriers to achieving socio-economic impacts;
3. Examining the stakeholder groups and sectors most likely to be impacted by blockchain;
4. Presenting insights into the nature and scale of the blockchain opportunity;
5. Using latest research to develop baseline forecasts to envisage how key blockchain opportunities might evolve without policy action at EU level;
6. Considering administrative burdens/costs and compliance burdens/costs;
7. Examining the impact of policy options on baseline blockchain forecasts and comparison of administrative costs with financial benefits that might arise from adopting policies;
8. Developing recommendations for monitoring and evaluation.

The preceding elements are similar to the European Commission's impact assessment methodology which form a key part of the Commission's better regulation agenda. This seeks to design and evaluate EU policies and laws so that they achieve their objectives in the most efficient and effective way.

To gather the required insights, meta-analysis methods have been used to review more than 100 reports and articles examining forecasts and the future impact of blockchain. There has been a profusion of blockchain articles in recent years. Many of these are relatively general, a few provide quantitative insights to current levels of investment and ICOs. Only a few provide forecasts for market growth and the impact of new business models. An area where there is a paucity of information concerns utility tokens. This has probably been caused by a lack of clarity in defining a 'utility token' and in providing functional and legal criteria for utility tokens.

[572] Demertzis M, Merler S, Wolff, G. 2018. Capital Markets Union and the fintech opportunity. Journal of Financial Regulation. 4,1. p157-165. http://www.guntramwolff.net/wp-content/uploads/2018/07/fintech.pdf (last accessed 22 January 2020).
[573] Body of European Regulators for Electronic Communications, https://berec.europa.eu/ (last accessed on 20 December 2019).

The next section of this chapter considers the underlying characteristics of blockchain by examining the capabilities provided by blockchain that can create new methods of providing goods and services. It also provides six distinct use cases where blockchain capabilities can create more efficient operations, support transformation and provide opportunities for new services and business models. The section also considers catalysts for blockchain development and the six key categories of benefits obtained from blockchain utilisation.

Section 6.3 examines barriers to blockchain development. These barriers have been found from secondary literature and from a Delphi method consultation which targeted more than 200 industry representatives, entrepreneurs, policy makers, economists, lawyers and other stakeholder groups. Almost 70 replies were received from online consultation and a workshop. It is these barriers and challenges that policymakers and legislators should address to alleviate problems and maximise benefits.

Section 6.4 provides insights to the nature and scale of blockchain impact in different industries and the key benefits of blockchain for different stakeholders. It also provides insights to blockchain development up until 2018.

Section 6.5 focuses on a forecast for the nature and scale of the blockchain opportunity up until 2030. The section considers appropriate forecasting methods and provides a rationale for using a variety of methods to triangulate predictions and communicate with experts. A note of caution is raised about enthusiastic forecasts and excited publicity by considering the hype cycle and the relatively low number of technologies in the past that have become productive. This section also used Delphi consultation to seek expert views about market forecasts for blockchain market expenditure and intra-EU trade facilitated by smart contracts. Two baseline forecasts from 2020 to 2030 are proposed, these represent how opportunities might evolve without EU policy action. The forecasts are used later in the Study as baselines against which to investigate potential policy impacts. The section also considers social and environmental impacts for blockchain.

Section 6.6 investigates costs associated with implementing the policies proposed in the previous chapter. Development of cost estimates is achieved by using European Commission Better Regulation Toolbox methods, particularly tools #59 and #60. 13 of 25 impact assessments that had been positively received by the Regulatory Scrutiny Board, from DG CONNECT and DG GROW between 2017 and 2019, were examined to provide insights into costs of policy implementation and policy impacts. The 13 assessments were selected because they adopted similar policies or operated in similar areas to this Study. This section also examined legislative timescales for items presented in the European Parliament to obtain insights into the likely timeline for the development of regulatory guidance measures and secondary legislation. The average time from first discussion in the European Parliament to implementation of the first policy elements was 24 months.

Having examined the costs of policies, the penultimate section investigates the potential impacts of policies. This provides insights into whether the impacts of policies are greater than their implementation costs. This section utilises insights provided about policy impacts and timelines for development in Section 6.6 to investigate potential impacts on the baseline forecasts developed after Delphi consultation in Section 6.5. This modelling method to estimate the different potential impacts of policies was possible for blockchain market expenditure and intra-EU trade facilitated by smart contracts. Insufficient insights were available in the poorly defined and rapidly developing area of utility tokens to utilise baseline modelling methods. Instead potential benefits from a handful of studies are compared with implementation costs. The section

concludes with a comparison of costs and potential socio-economic benefits that reveals benefits significantly outweigh policy implementation costs.

The final section examines previous impact assessments that have been approved by the Regulatory Scrutiny Board to draw out best practice methods for monitoring and evaluating policies in this report, if they are introduced.

6.2. Blockchain opportunities and catalysts

Blockchain opportunities are achieved through the unique combination of capabilities provided by the software. It is these capabilities that can be utilised in different ways to provide stakeholder benefits. This section considers these capabilities and the key use cases that they facilitate. The key catalysts and key benefits driving blockchain are also examined.

6.2.1. Blockchain capabilities

Blockchain and distributed ledger technologies are an innovative combination of technical components that share the same conceptual origin. There is a difference between the two terms despite the fact that many people us them interchangeably[574]:

- A *distributed ledger* is a database that exists and is replicated across several locations or among multiple participants. The distinctive factor of a DLT is that consensus among these different servers or participants is achieved without relying on a central authority. A distributed ledger can eliminate the need for a central authority or an intermediary to process, validate and/or authenticate transactions;
- *Blockchain* is a specific type of distributed ledger with a distinct set of operational processes. Unlike other distributed ledgers, blockchains package transactions or sets of data into cryptographic hash-linked blocks in a sequential chain. These blocks are very difficult to reverse, append-only and can be used to create and document a history of transactions being made of the items being recorded.

Blockchain, like many new technologies, provides 'capabilities' which will enable opportunities to carry out activities and operations in new ways. It is useful at this point to differentiate the underlying principles of blockchain technologies from the operational capabilities it provides for many users. Separating the two elements is important in the context of this Study. The technology simply manipulates data, in itself the technology has no value. It is the capabilities provided by the technology that produce benefits for businesses, other organisations, citizens and society. These capabilities have benefits and impacts that this Study is trying to measure so that the impact of policies[575] can be compared with baseline forecasts and current expectations.

Blockchain technology and software is used to synchronise data stored in a distributed manner amongst peers on all the computers or servers ('nodes') participating in a particular network. A key advantage, provided by the way blockchain records information on a digital and distributed ledger, is the identical transparent manner that creates trust in the 'ordering' of information, data and transactions recorded.

Trust is created because all the nodes in the network control, check and consent to any additions or changes to the recorded data. Blockchain can thus be used for record keeping, transferring values (via cryptocurrencies or otherwise) and smart contracts to

[574] In the remainder of this chapter, to create simplicity, the short term 'blockchain' is used. But where required the precise definitions are adhered to.
[575] To reduce barriers to benefits realisation, alleviate problems and ensure legal and ethical operations.

automatically execute a transaction when one or more precondition is met.[576] A blockchain allows participants to share data and code without the need for intermediaries to operate or maintain the service. All parties share the same data, which is replicated across all the nodes in the network.

McKinsey notes that there are six distinct use cases where blockchain capabilities can create more efficient operations, support transformation and provide opportunities for new services and business models.[577] Three of the capabilities concern static information storage, these include:

- *A static registry* - this use case largely concerns a distributed database for storing reference data such as land titles and patents;
- *Identity information* - this use case focuses on distributed databases with identity-related information. Examples include civil registry and identity records and use in voting;
- *Smart contracts* - this use case concerns conditions recorded on a blockchain, triggering automated, self-executing actions when these predefined conditions are met. Examples include cash-equity trading and new-music release.

A higher magnitude of benefits is likely to arise from the use of blockchain in transactions where registries are created of tradeable information. McKinsey identify two capabilities concerning transactions:

- *Dynamic registry* - this use case focuses on dynamic distributed databases that are timestamped and updated as assets are exchanged on the digital platform. Examples include fractional investing and drug supply chains;
- *Payments infrastructure* - this use case concerns dynamic distributed databases that update as cash or cryptocurrency payments are made among participants. Examples include cross border peer-to-peer payment and insurance claims.

The McKinsey study also has a sixth 'catch-all' category concerning cases composed of several of the previous examples and other uses, these include tokenisation and blockchain-as-a-service (BaaS). Blockchain capabilities provide the ability to convert rights for an asset into a digital token. An asset (e.g. a property, financial bond, artwork or diamonds) can be tokenised. This creates a digital representation that lives on blockchain. Blockchain guarantees that ownership information is difficult to change.[578] The feedback received during the workshop for this Study noted the complexity and subtle differences in nearly all areas of blockchain activity. The adoption by McKinsey of a 'catch all' category covering a multitude of activities is therefore problematical. To include utility tokens within this group creates further complexity since many at the

[576] Deloitte, 'Blockchain: Legal implications, questions, opportunities and risks' (2018), https://www2.deloitte.com/global/en/pages/legal/articles/2018-legal-blockchain.html (last accessed on 20 December 2019).
[577] McKinsey, 'Blockchain beyond the hype: What is the strategic business value?' (2018), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value (last accessed on 20 December 2019).
[578] This approach sounds simple, but a constraint to widespread use is that there are not currently regulations concerning blockchain capabilities and cryptocurrencies. Currently token owners just own tokens. They generally have no legal rights on an asset and thus are not protected by law. The level of rights is generally determined by the token. Legal changes are required to facilitate these new business models. Sazandrishvili G., 'Asset tokenisation on blockchain explained in plain English' (2018), https://medium.com/coinmonks/asset-tokenization-on-blockchain-explained-in-plain-english-f4e4b5e26a6d (last accessed on 20 December 2019).

workshop suggested it was impossible to adopt a legal definition of a utility token based on functional criteria.

A simple illustration of the use of blockchain capabilities in supply chain transactions provides a useful insight to the many ways in which blockchain can be developed and the complexities that can arise with different use cases. This Study therefore focuses on expenditure on blockchain, as this provides insights to the general growth of the technology. Two broad use cases have also been adopted for closer examination; these include:

- The use of smart contracts in intra-EU28 trade in goods;
- The development of utility tokens.

Two, often quoted, examples provide real world examples of blockchain use. In the drug industry, blockchain allows complete traceability from a product's origin to purchase by the final recipient.[579] At a factory where a drug is manufactured it can be recorded using RFID, barcode or other technology. This would be registered as the first block in the chain. Having checked against block one, the second block would record the drug's updated status as it is moved along the supply chain. Permissions built into the blockchain would limit its onward sale to approved trading partners. All those involved in transactions can track and trace the product in the supply chain to exclude the risk of grey imports.[580] Walmart has already started to use blockchain in the supply chain to track the provenance of mangoes as they are shipped from Mexico to the United States and to track its pork supply chain in China.[581] The company says its distributed ledger has shortened the time to track produce from six days to two seconds, which helps solve several problems regarding food safety, customs and regulatory filings, and automated payments.[582]

6.2.2. Blockchain benefits

The capabilities, described in the previous section, provided by blockchain will be used in many different environments to provide a variety of benefits. Literature[583] has identified six key categories of benefits:

- *Trust and Integrity* - when everything is archived and authorised in a decentralised way, the system ensures that data is carried out and processed in a reliable and transparent manner;[584]

[579] Op.cit, Deloitte, 'Blockchain: Legal implications, questions, opportunities and risks' (2018).
[580] Niels Hackius and Moritz Petersen, 'Blockchain in logistics and supply chain: Trick or treat' (2017), Proceedings of the Hamburg International Conference of Logistics, available at https://pdfs.semanticscholar.org/7752/f1275da69d208e5a76d7adc6b12b3b61699e.pdf (last accessed on 20 December 2019).
[581] Teppo Felin and Karim Lakhani, 'What problems will you solve with blockchain' (September 2018), MIT Sloan Management Review, https://sloanreview.mit.edu/article/what-problems-will-you-solve-with-blockchain/ (last accessed on 20 December 2019).
[582] Ana Alexandre, 'Walmart is ready to use blockchain for its live food business (April 2018), https://cointelegraph.com/news/walmart-is-ready-to-use-blockchain-for-its-live-food-business (last accessed on 20 December 2019).
[583] IBM, 'Emerging technology projection: The total economic impact of IBM blockchain: Projected Cost Savings And Business Benefits Enabled By IBM Blockchain' (July 2018), available at https://www.ibm.com/downloads/cas/QJ4XA0MD (last accessed on 20 December 2019).
[584] Michael Pisa and Matt Juden, 'Blockchain and economic development: Hype vs. reality' (July 2017), CGD Policy Paper. Washington, DC: Center for Global Development. Available at https://www.cgdev.org/publication/blockchain-and-economic-development-hype-vs-reality (last accessed on 20 December 2019).

- *Transparency* - blockchain is an open source technology operated by a set of actors called miners. In a distributed ledger every transaction is recorded publicly.[585] Public verifiability allows anyone to verify correct system working;
- *Immutability* - a third-party cannot easily make any changes to the system;
- *Security* - with no central point to be exploited, the system is protected against hacking attacks and fraud;
- *Reduced transactions costs* - blockchain allows peer-to-peer and business-to-business transactions to be completed without the need for third party intermediaries;
- *Innovation* - completely new business models and services can be developed.

However, some of these benefits have been questioned.[586] For example:

- *Trust and integrity* will only be assured when regulations or third parties are able to legally validate transactions;[587]
- *Transparency* has been questioned because some participants use pseudonyms and thorough checks on the identity of participants are rarely undertaken;[588]
- *Security* has suggested coding flaws may compromise the security of blockchain;[589]
- *Reduced transaction costs* cost efficiency is open to question when the volume of computing power used in a highly distributed network is taken into account.

Many of the benefits that are forecast to arise from blockchain are based on the notion of disintermediation. At present, many markets operate through intermediaries (e.g. banks, credit card companies or other agents), they need to be paid for their services, network effects give them information that enables them to consolidate their market power.

Blockchain provides a means for communal ownership and maintenance of financial records. It provides a new way for strangers/traders to collaborate without the need to trust an intermediary or centralised authority.[590]

Blockchain appears to offer clear advantages. However, commentators have noted that intermediaries play a role beyond simple record keeping. They can rectify mistakes, resolve disputes and if a banking passcode is lost, the intermediary can provide a new one. If a Bitcoin passcode is lost there is no intermediary to provide support and if the passcode is not found Bitcoin assets will be lost forever.

---

[585] For clarification, it is actually the nodes (or 'auditors') that are the primary operators. Miners ('record producers') are responsible for ordering transactions.
[586] Op.cit, Deloitte, 'Blockchain: Legal implications, questions, opportunities and risks' (2018).
[587] Darcy Allen, Alastair Berg, Chris Berg, Brendan Markey-Towler, and Jason Potts, 'Some Economic Consequences of the GDPR' (March 29, 2019), Economics Bulletin, vol. 39, no. 2, p.785-797. Available at SSRN: https://ssrn.com/abstract=3160404 or http://dx.doi.org/10.2139/ssrn.3160404 (last accessed on 20 December 2019).
[588] This elements is affected by whether public or private blockchains are being examined. Thorsten Koeppl and Jeremy Kronick, 'Blockchain technology: What is instore for Canada's economy and financial markets'(2017), CD Howe Institute Commentary No. 468, available at https://www.cryptoninjas.net/wp-content/uploads/2017/09/Commentary_468_0.pdf (last accessed on 20 December 2019).
[589] Mike Orcutt, 'Once hailed as unhackable, blockchains are now getting hacked' (Feb 2019), MIT Technology Review, https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/ (last accessed on 20 December 2019) and McKinsey, ' Blockchain beyond the hype: What is the strategic business value? (2018), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value (last accessed on 20 December 2019).
[590] Christian Catalini and Joshua S. Gans, Some Simple Economics of the Blockchain (April 20, 2019). Rotman School of Management Working Paper No. 2874598; MIT Sloan Research Paper No. 5191-16. Available at SSRN: https://ssrn.com/abstract=2874598 or http://dx.doi.org/10.2139/ssrn.2874598 (last accessed on 20 December 2019).

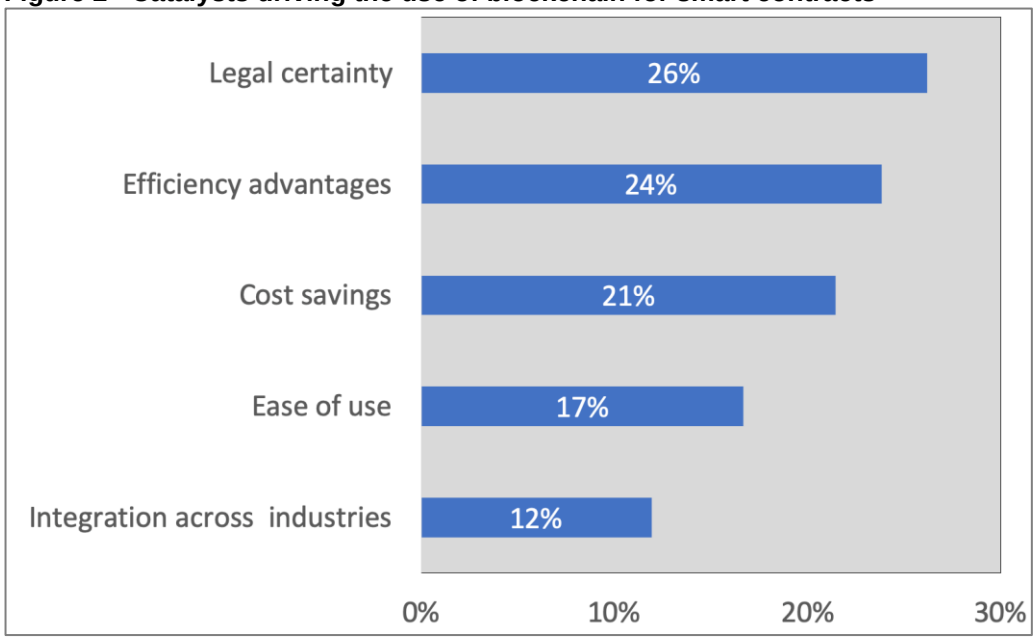
Policy development for blockchain must support EU trade policy and increase trading opportunities for EU companies by removing trade barriers and by guaranteeing fair competition.[591] This is essential for the European economy as it affects growth and employment.[592] Policy development to support blockchain development must have clear focused goals and objectives so that outcomes and impacts can be articulated and then investigated in impact assessments and eventually monitored after the implementation of policies. Policies should focus on supporting and enhancing catalysts for development and clearly address barriers to blockchain development. The next sections therefore provide an overview of these catalysts and barriers.

6.2.3. Blockchain catalysts

The lists of benefits provided in the previous section could be regarded as catalysts. However, as the previous section also noted, it is possible that not all the benefits will be achieved. We therefore examined perceived catalysts more closely.

During the research, we contact more than 200 blockchain experts and asked them about the catalysts for development.[593] To try and provide a little precision, in a complex array of use cases where blockchain can be utilised, we asked the experts to provide insights into the catalysts driving the use of blockchain for smart contracts.

Figure 2 - Catalysts driving the use of blockchain for smart contracts



[591] European Parliament, 'Making the Most of Globalization: EU Trade Policy explained (June 2019), https://www.europarl.europa.eu/news/en/headlines/economy/20190528STO53303/making-the-most-of-globalisation-eu-trade-policy-explained (last accessed on 20 December 2019).
[592] Chief Economist Note, 'How important are EU exports for jobs in the EU?' (Nov 2018), available at http://trade.ec.europa.eu/doclib/docs/2018/november/tradoc_157517.pdf (last accessed on 20 December 2019).
[593] The list of blockchain experts was derived from Commission contact lists, our teams' knowledge of key experts and online research. The 200 (plus) experts were invited to a concluding workshop in Brussels on 2 December 2019. Nearly 30 replies to a briefing paper and questionnaire were received from experts unable to attend the workshop. In addition, just over 40 people at the workshop responded to the questionnaire. In total 70 expert replies were received. Not all respondents answered all questions. Their viewpoints are provide in Figure 2 and other locations in this chapter. Responses from the two sets of respondents (prior to the workshop and during the workshop) were not weighted because they were drawn from the same original sample frame.

The most significant catalyst concerns one of the key foci for this Study – legal certainty (see Figure 2). During the research, 'legal certainty' and 'regulation clarity' were regarded as key catalysts. Interestingly, since this certainty and clarity does not currently exist in all areas, they were also included as key barriers by some observers.

The second and third catalysts in Figure 2 both relate to the key monetary benefit associated with reduced transactions costs identified in the previous section.

6.3. Barriers to blockchain

The previous section concluded with catalysts for blockchain adoption. This section examines the opposing factors – barriers. It is these barriers and challenges that policymakers and legislators could address to alleviate problems and maximise benefits.

McKinsey highlight three key issues concerning blockchain:[594]

- Blockchain is still three to five years away from feasibility at scale, primarily because of the difficulty of resolving the 'coopetition' paradox to establish common standards;
- Blockchain's short-term value will be predominantly in reducing cost before creating transformative business models;
- Blockchain does not have to be a disintermediator to generate value, a fact that encourages permissioned commercial applications.

These three observations provide a useful note of caution in an area where there is a lot of hype about blockchain impacts and forecasts for growth. Section 6.5 investigates this hype and blockchain forecasts in more detail.

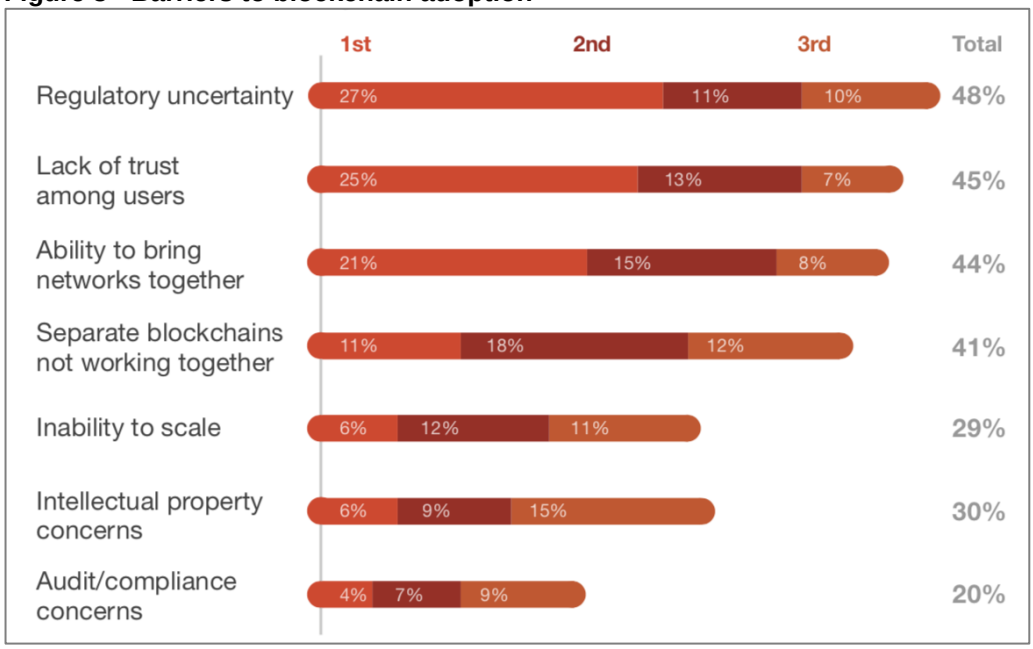
Effective utilisation of blockchain technologies faces a number of challenges.[595] These include:

- *Awareness and understanding* - One of the main challenges associated with blockchain is a lack of awareness of the technology, and a widespread lack of understanding of how it works, causing companies to neglect investments in this technology. Users also face implementation difficulties. Blockchain uses complex software that is not user-friendly and requires a good understanding of the blockchain's underlying processes;
- *Data privacy and confidentiality* are potential risks, since the ledger may be distributed to all participants, meaning that every node of the network can potentially access and read all the records. Moreover, there are still some security concerns about blockchains, even if some solutions have been developed giving restricted access to information;
- *Standardisation* - There is currently a lack of standardisation in the use of blockchain technology and the development of smart contracts. Indeed, there is no regulatory framework or industry standard associated with the use of blockchain technology;
- *Technical challenges* that need to be addressed with blockchain technology include scalability and computing power requirements to support higher volumes of use with an increasing number of transactions per second.

[594] Op.cit, McKinsey, 'Blockchain beyond the hype: What is the strategic business value?' (2018).
[595] Melanie Swan, 'Anticipating the economic benefits of blockchain' (October 2017), Technology Innovation Management Review, vol. 7, issue 10. p.6 -14. Available at https://timreview.ca/sites/default/files/Issue_PDF/TIMReview_October2017.pdf (last accessed on 20 December 2019).

PwC's 2018 global blockchain business survey identified the seven biggest barriers to blockchain adoption (see Figure 3), providing an overview of respondents top three challenges.[596]

Figure 3 - Barriers to blockchain adoption

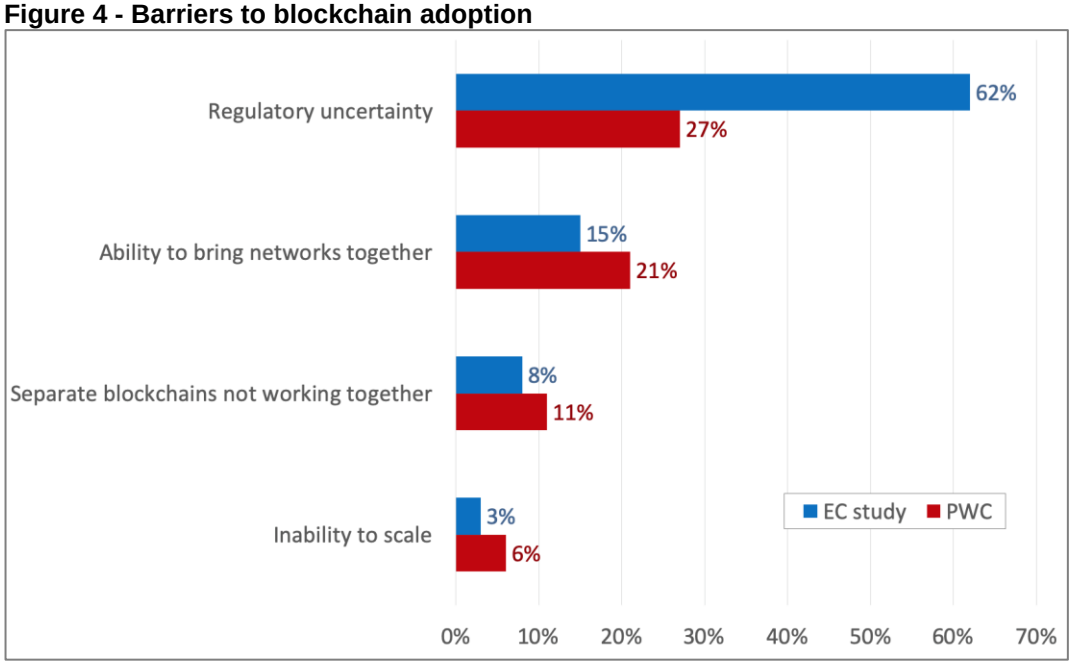


PwC undertook a global study of business-people. During engagement activities for this Study, our team asked the EU28 experts we approached for their views about barriers to blockchain adoption. It is likely that the results in Figure 4 partially reflect the two different viewpoints of the constituent groups contacted by the two studies.[597] PwC approached business-people and our Study contacted more general blockchain experts, many of whom had an interest in legal issues.

[596] PwC, 'Global blockchain business survey: Blockchain is here what is your next move?' (2018), available at http://explore.pwc.com/blockchain/Exec-summary?WT.mc_id=CT11-PL1000-DM2-TR1-LS4-ND30-TTA5-CN_US-GX-xLoSBlockchain-LB-PwCExecSum&eq=CT11-PL1000-DM2-CN_US-GX-xLoSBlockchain-LB-PwCExecSum (last accessed on 20 December 2019).

[597] EU28 respondents were only asked for their single largest barrier to the development of smart contracts. Therefore Figure 4 only presents the largest challenge identified by their PwC counterparts. Total for groups do not add to 100 per cent because other elements with values below the lowest quoted in the Figure 4 were not included.

Figure 4 - Barriers to blockchain adoption



It would be unwise to place too much emphasis on similarities and differences between the two studies. The difference in regulatory uncertainty probably represents differences in the importance of this issue for the two constituencies. The magnitude of other differences is similar between the two studies.

6.4. Stakeholder groups and sectors impacted by blockchain and recent trends

It was noted in Section 6.2 that blockchain technologies and capabilities can be used in many different ways for different activities and use cases.[598] The UK Government Chief Scientific Adviser[599] emphasised that distributed ledger technology has the potential to underpin a new technological revolution. This view was asserted on the basis that distributed ledger technologies represent an innovation towards the radical end of the change spectrum because of their potential to impact a broad extent of areas in the business model: from new products and services, through operating systems and organisational structures, to the sheer number of potential industries that could be affected.

This section provides insights into the nature and scale of blockchain impact in different industries and the key benefits of blockchain for different stakeholders. It also provides insights into blockchain development up until 2018.

[598] Forbes, 'Blockchains value isn't currency, It's technology' (July 2015), https://www.forbes.com/sites/robertrosenkranz/2015/07/07/bitcoins-value-isnt-currency-its-technology/#6bb33fe11f11 (last accessed on 20 December 2019) and Sinclair Davidson, Primavera De Filippi, Primavera and Jason Potts, 'Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology' (July 19, 2016). Available at SSRN: https://ssrn.com/abstract=2811995 or http://dx.doi.org/10.2139/ssrn.2811995 (last accessed on 20 December 2019).

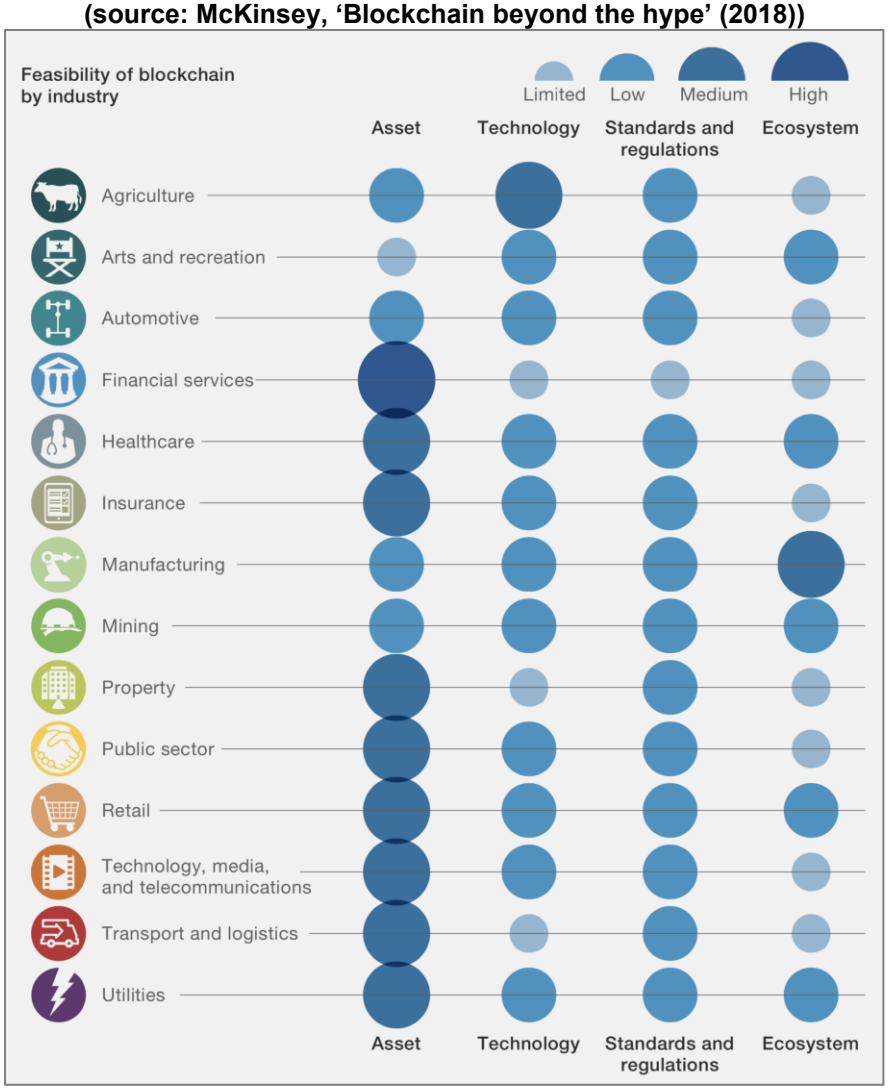
[599] UK Government Chief Scientific Adviser, 'Distributed Ledger Technology: Beyond Blockchain '(Jan 2016), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (last accessed on 20 December 2019).

6.4.1. Sectoral impacts and benefits

McKinsey provided an overview of the benefit of blockchain by sector.[600] Their analysis evaluated more than 90 potential use cases against the four key factors that determine a use case's feasibility in a given industry. These include standards and regulations, technology, asset, and ecosystem (see Figure 5). McKinsey found that the lack of common standards and clear regulations are a major limitation on blockchain applications' ability to scale. However, where there is strong demand and commitment, work is already under way to resolve this issue. Standards can be established with relative ease if there is a single dominant player or a government agency that can mandate the legal standing.

They also found that asset type determines the feasibility of improving record keeping or transacting via blockchain. A key factor is the digitisation potential of the asset. Assets like equities, which are digitally recorded and transacted, can be managed end-to-end on a blockchain system. However, connecting and securing physical goods to a blockchain requires enabling technologies like IoT and biometrics.

Figure 5 - Feasibility and sectoral impact of blockchain (source: McKinsey, 'Blockchain beyond the hype' (2018))



[600] Op.cit, McKinsey, 'Blockchain beyond the hype: What is the strategic business value?' (2018).

Figure 5 highlights that the largest blockchain impacts are likely to be found in the financial services sector. This is also the sector where the three other factors (technology, standards and regulations, and ecosystem) are perceived the lowest constraints on development.[601]

The World Economic Forum have undertaken a review of the benefits of blockchain for different sectors (see Figure 6)[602]. Overall, WEF assert that blockchain adds value where there is a need for tamper-evident ledgers along with distributed control, particularly where participants have an even hierarchy. The WEF study also highlights differences in benefits arising from blockchain for 13 industrial sectors. The number in the blue boxes indicate the relative importance of the eight benefits/capabilities in the left-hand vertical column - one indicates the most important benefit, eight the least important.

Figure 6 - Blockchain benefits in different sectors (source: the World Economic Forum, 'Building value with blockchain technology' (2019))

		Automotive	Banking	Comms & media	Consumer goods & services	Energy	Healthcare	High tech	Insurance	Public service	Retail	Software & platforms	Travel	Utilities
1	Full traceability of any information on the blockchain	7	2	4	3	1	1	3	1	3	1	6	1	4
2	Ability to ensure data has not been tampered with	4	1	1	3	4	2	1	2	1	5	2	2	4
3	Distributed nature of the technology	8	4	5	1	8	4	3	3	4	6	4	3	6
4	Smart contracts and automation	2	3	2	2	5	5	6	4	6	3	3	6	3
5	Increased speed and efficiency	3	6	2	5	3	7	7	7	2	4	5	5	1
6	Increased security	1	6	7	7	2	3	1	5	4	2	1	3	2
7	A holistic view with transparency for all appropriate parties	5	5	6	6	5	6	5	5	6	7	7	7	7
8	New business products or services	6	8	8	8	7	8	8	8	8	7	7	8	8

It is immediately evident that the key benefits/capabilities are the 'full traceability of any information on the blockchain' (the most important benefit for five of the 13 sectors examined) and the 'ability to ensure data has not been tampered with' (most important benefit in four sectors and also second most important in four sectors).

6.4.2. Financial services

The preceding section highlighted that a number of studies forecast that blockchain will have the largest impact in the financial services sector. A short review of the sector helps to better understand the significance of preceding issues such as blockchain capabilities, catalysts, barriers and disintermediation. A more fulsome examination of socio-economic impacts is provided in Section 6.5.

The World Economic Forum (WEF) highlights that many liquid and illiquid financial assets remain highly dependent on intermediating institutions to discover and connect buyers and sellers, often based on networks of pre-existing relationships with other

[601] As indicated by the small size of the blue graphics in these columns.
[602] The World Economic Forum 'Building value with blockchain technology: How to evaluate blockchains benefits' (July 2019), available at http://www3.weforum.org/docs/WEF_Building_Value_with_Blockchain.pdf (last accessed on 20 December 2019).

institutions.[603] For example, WEF[604] highlights that financial services will be transformed by blockchain technology with expectations of at least 10 per cent of global GDP being stored on blockchain platforms by 2027.

The World Bank estimated Global GDP to be €74 trillion in 2018.[605] Statista forecast that global GDP will reach €96 trillion in 2024.[606] Linear extrapolation suggests the figure would reach €106 trillion in 2027. One can therefore assume that the WEF estimate of 10 per cent would equate to €10.6 trillion in 2027.

West estimated the market valuation[607] of cryptocurrencies was €775 billion in 2018. The forecast CAGR of 11.9 per cent for the global cryptocurrencies market between 2019 to 2024.[608] This extrapolation suggests growth in market valuations to €1.5 trillion in 2024, reaching €2.1 trillion in 2027.[609]

To achieve the WEF estimate of €10.6 trillion global GDP stored on blockchain in 2027, CAGR in the value of cryptocurrencies would need to reach 33.7 per cent. The WEF estimated CAGR is almost three times the West forecast. This is one example of hype and caution that must accompany early technology development.

McKinsey[610] reports that approximately 90 per cent of major European, and North American banks are already experimenting or investing in blockchain. According to EY, fintech investments are surging,[611] reaching €27 billion worldwide in 2017 alone, with €4.6 billion in Europe (17 per cent of global investment) making this more than double the amount of a year before. Over half of this investment occurred in the business-to-business space.[612]

Blockchain capabilities have the potential to support market making and disintermediation. A number of financial platforms are emerging that realign how buyers and sellers are connected for various products and transactions, generally improving the efficiency of those markets. These new platforms provide increased visibility and control over transactions by buyers and sellers. Key benefits include:

- *Transparency* – Buyers and sellers gain more visibility throughout the transaction process and are therefore able to exert greater control over the

[603] The World Economic Forum, 'The Future of Financial Services - How disruptive innovations are reshaping the way financial services are structured, provisioned and consumed' (June 2015), available at http://www3.weforum.org/docs/WEF_The_future__of_financial_services.pdf (last accessed on 20 December 2019).
[604] Ibidem.
[605] World Bank, Global GDP (2019), https://data.worldbank.org/indicator/NY.GDP.MKTP.CD. Calculated at a mid-2018 US$ to € exchange rate of 0.862.
[606] Statista, 'Global gross domestic product (GDP) at current prices from 2014 to 2024' (2019), https://www.statista.com/statistics/268750/global-gross-domestic-product-gdp/ (last accessed on 20 December 2019).
[607] Market valuation is thought to be the total market value of all cryptocurrencies in 2018. White and Case figures probably relate to the initial share of the currency received by currency developers.
[608] West, 'The World Market for Cryptocurrency: 2017-2018 Review & 2019-2024 Forecast' (Sept 2019), https://www.globenewswire.com/news-release/2019/09/09/1912565/0/en/The-World-Market-for-Cryptocurrency-2017-2018-Review-2019-2024-Forecast-with-Analysis-on-Bitmain-Technologies-BitGo-NVIDIA-Corporation-Ripple-Networks-and-Coinbase.html (last accessed on 20 December 2019).
[609] It is important to highlight that one should separate the value of cryptoassets native to public blockchains with the value created through business usage of permissioned blockchains. As later sections of this chapter emphasise they are not directly comparable.
[610] Op.cit, McKinsey, 'Blockchain beyond the hype: What is the strategic business value?' (2018).
[611] Blockchain companies and projects constitute only a small proportion of the total FinTech market.
[612] EY, Global Banking Outlook (2018), available at https://www.ey.com/Publication/vwLUAssets/ey-global-banking-outlook-2018/$File/ey-global-banking-outlook-2018.pdf (last accessed on 20 December 2019).

transactions and reduce the opportunities for suboptimal transactions by intermediaries;
- *Improved access* - The ability to buy / sell financial assets and products is less dependent on the scale or the size of the intermediaries' network, improving access to the market by more buyers, sellers, and intermediaries;
- *Faster, cheaper transactions* - As the discovery and assessment of counterparties become more streamlined and automated, the efficiency of intermediaries or new platforms will improve, leading to faster turnaround and lower cost to complete transactions for buyers and sellers.

Because blockchain technologies disintermediate the fund value chain, some functions and activities may not be needed in the future. This will lead to reductions in the time taken to execute the transfers of value.[613] Currently, the time to exchange fund share versus payment is two or three days, in the future this could occur almost instantaneously. In a full implementation of the technology, fund promoters could simply directly distribute fund shares without any intermediary. Even the assets side could be taken over by blockchain, supplanting custodian banks and fund accounting firms.

Accenture Clearstream[614] estimates that internal fragmentation (i.e. inefficiencies specific to individual banking institutions) of the global collateral management market costs more than €4 billion annually. They note that external costs and potential savings of reorganisation and utilisation of technology are difficult to estimate because they are dependent upon future regulation, but our survey suggested that cost savings could well be considerable. They noted that the highest potential cost savings can be achieved through implementing comprehensive IT solutions to develop a single application, providing a complete overview of collateral across all asset classes, business divisions and legal entities.

A Santander Innoventures report[615] asserts distributed ledger technology could reduce banks' infrastructure costs attributable to cross-border payments, securities trading and regulatory compliance by between €13.8 to €18.4 billion per annum by 2022.[616] Blockchain technology carries the potential to disrupt many industries, especially the financial industry.[617] It would make trading and post-trading processes much more efficient, improve regulatory control, and remove multiple intermediaries. The technology enables transactions to be more transparent, nearly instantaneous, and without the need to trust a central party.

A study undertaken by Deloitte[618] examines the impact of blockchain technology in Luxembourg which, with €3.5 trillion in 2015, made Luxembourg the largest European financial centre and second largest player in the world in terms of local fund assets. The study highlighted that activities are performed through intermediaries and trusted counterparties which add to transaction costs. Deloitte estimated the processing costs

[613] Op.cit., Deloitte, 'Blockchain: Impacts of the blockchain on fund distribution' (2018).
[614] Accenture-Clearstream, 'Collateral Management – Unlocking the Potential in Collateral' (2011), available at https://www.clearstream.com/resource/blob/1316326/e5bf3b589c8f3ff6afd19166f9d53d3b/accenture-collateral-report-pdf-data.pdf (last accessed on 20 December 2019).
[615] Santander Innoventures, 'The Fintech 2.0 Paper: Rebooting financial services' (2015), available at http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf (last accessed 20 December 2019).
[616] Stafford P, 'FT Explainer: The blockchain an financial markets' (2015), https://www.ft.com/content/454be1c8-2577-11e5-9c4e-a775d2b173ca (last accessed on 20 December 2019).
[617] Op.cit, Deloitte, 'Blockchain: Impacts of the blockchain on fund distribution' (2018).
[618] Deloitte and Fundsquare, 'Europe's funds expenses at a crossroads: The benefits of mutualising the cost of distribution' (2015), available at https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/IM/lu-en-europe-fund-expenses-survey-24062015.pdf (last accessed on 20 December 2019).

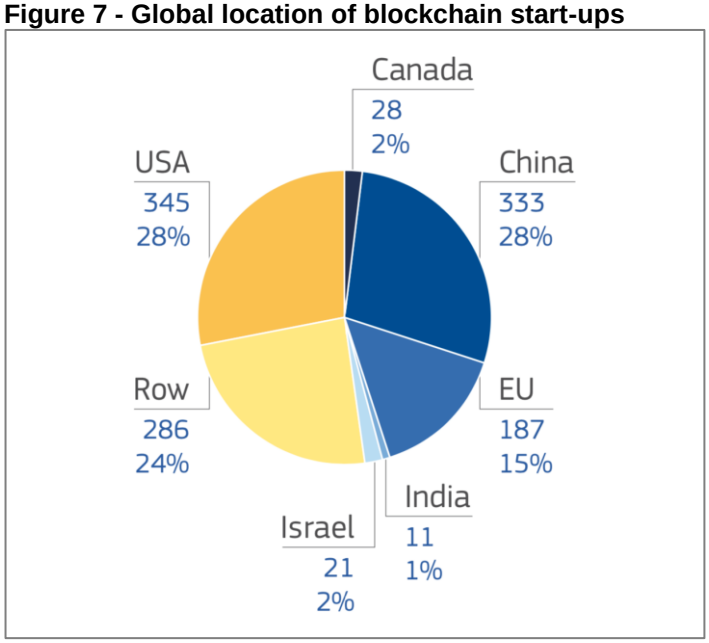
of fund distribution in Luxembourg in 2014 were €1.2 billion. In addition, they found that 23 per cent of the fund order process is still handled manually. Deloitte estimates that by automating processes and removing the need for intermediaries, blockchain could improve distribution process speed, efficiency and reduce costs. However, this could be at the expense of losing many jobs in Luxembourg, where the fund industry employed 14,000 people in 2015.

6.4.3. Trends in blockchain

Market oriented information about blockchain growth and trends largely relates to expenditure on blockchain solutions, trends in blockchain start-ups and funding for start-ups. These are examined below.

IDC[619] estimated that worldwide spending on blockchain solutions reached €2.48 billion in 2018. Forecasts for growth in spending to 2030 are provided in Section 6.5.3. JRC[620] estimates that as of 31 December 2018, the largest number of blockchain firms was established in the USA, followed by China. The EU lags in this classification with only 15 per cent of the global blockchain start-up ecosystem (see Figure 7). Within Europe, the UK is estimated to have 89 (48 per cent) of the 187 start-ups. Germany has 16 (eight per cent) and France 13 (seven per cent). All other EU countries have less than ten start-ups.

Figure 7 - Global location of blockchain start-ups



The number of start-ups is interesting, but this provides little insight into activities. A better insight into the intensity of activities is probably best obtained from looking at the level of investment in start-ups. JRC[621] estimated the volume of funding provided to blockchain start-ups between 2009 and 2018. They found that US firms received the most funding, totalling €4.4 billion. Companies from the EU received €2.9 billion in investments, followed closely by start-ups from China (€2.8 billion) (see Figure 8).

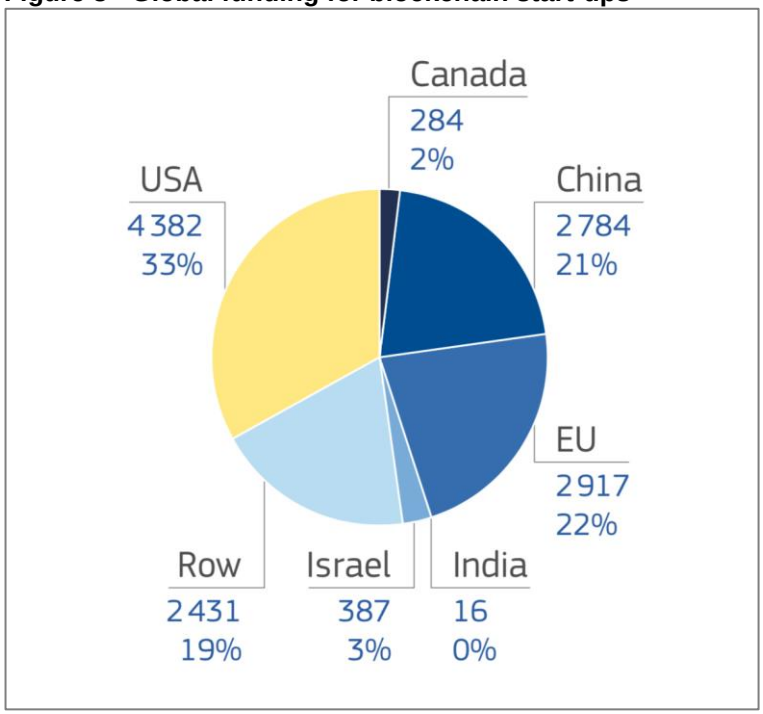
[619] IDC, Worldwide Semiannual Blockchain Spending Guide (2019), available at https://www.idc.com/getdoc.jsp?containerId=IDC_P37345. The study forecast was US$2.9 billion. This figure was estimated in euros using the exchange rate prevailing at the mid-point of the year for the forecast (1 July 2018; exchange rate 0.8554)

[620] JRC, 'Blockchain now and tomorrow' (2019), https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-now-and-tomorrow (last accessed on 24 January 2020), p. 31.

[621] Ibidem, p.34.

Overall, the global level of funding of all types, including venture source, grants and ICOs exceeded €13.1 billion.

Figure 8 - Global funding for blockchain start-ups



Within Europe, funding for UK blockchain start-ups between 2009 and 2018 was estimated to be €2.03 billion (69 per cent of funding in the EU). The Netherlands had the second highest level of funding, €352 million (12 per cent). Next was France with €167 million (6 per cent).

The estimates in this section reveal high levels of activity and investment, but they do not provide forecasts to 2030 and insights to the impact of blockchain in the three key areas of interest to this Study (blockchain market growth, the use of smart contracts in intra-EU28 trade in goods and the development of utility tokens). These forecasts are required to provide a baseline against which the need for and the impacts of policy options might be assessed. The next section provides an introduction to the forecasting parameters and methods that have been used to underpin this Study. Section 6.5.3 provides a note of caution about the hype and anticipation that can sometimes be associated with forecasts concerning new technologies.

This short overview has provided insights to the size of the EU28 blockchain sector. These include:

- 15 per cent of global start-ups;[622]
- 17 per cent of global fintech investments;[623]
- 22 per cent of global funding for start-ups.[624]

These proportions provide a basis for triangulation with later analysis and they align well with further insights in the next section.

[622] Ibidem.
[623] Op.cit, McKinsey, 'Blockchain beyond the hype: What is the strategic business value?' (2018).
[624] Op.cit, JRC, 'Blockchain now and tomorrow' (2019).

6.5. Insights to the nature and scale of the blockchain opportunity

This section focuses on the methods used to forecast the nature and scale of the blockchain opportunity. The next section presents details of best practice principles for forecasting and introduces key methodologies used in this study. Section 6.5.3 describes how these principles and parameters were used to develop forecasts for blockchain market growth and the use of smart contracts.

6.5.1. Forecasting consideration and methods

At the core of the socio-economic impact element of this Study, is the requirement to develop the best possible forecasts for blockchain utilisation in three areas up until 2030. Desk research reviewed a number of prediction methodologies[625] and forecasting checklists.[626] These have provided a robust methodological underpinning to the Study. Carnegie Mellon University developed a useful overview of key elements that can help to make forecasts more reliable. Their relatively simple checklist[627] has provided a solid foundation for this Study:

- Forecasting should be a continuous process;
- Forecast accuracy is dependent upon the planning horizon;
- A proper forecast requires communication. Engage others in the process;
- A forecast is never 100 per cent accurate.

To ensure extensive consultation, forecasts have been shared with more than 200 blockchain experts and at a workshop, hosted by the Commission and the Consortium on 2 December 2019. More than 60 experts attended the workshop in Brussels. In addition, our team have contacted experts and relevant stakeholder organisations for more detailed information throughout the Study. Experts included individuals developing blockchain technologies and promoting the use of blockchain, and organisations primarily focused on those representing blockchain businesses in Europe and the US. Interviews, emails and questionnaires identified key barriers and catalysts for growth, blockchain impacts and forecasts.

The planning horizon is 2030. Of course, as the horizon extends forecasts will be more speculative. For example, it is entirely possible if not likely that there will be major users of blockchain in 2030 that are not important or do not exist today.

[625] Armstrong J, 'Principles of Forecasting: A Handbook for Researchers and Practitioners' (2002), (International Series in Operations Research & Management Science). Springer Science ; Hyndman R and Athanasopoulos G, 'Forecasting principles and practice' (2013). Otexts.org ; Silver N., 'The Signal and the Noise: Why So Many Predictions Fail--but Some Don't' (2015), Penguin. Makridakis et al., 'Objectivity, reproducibility and replicability' (2018), in forecasting research. Available at https://www.researchgate.net/profile/Evangelos_Spiliotis/publication/325731015_Objectivity_reproducibility_and_replicability_in_forecasting_research/links/5b59bfbe458515c4b249d774/Objectivity-reproducibility-and-replicability-in-forecasting-research.pdf (last accessed on 20 December 2019).

[626] Armstrong J S, 'Forecasting standards checklist' (2001), available at http://www.forecastingprinciples.com/files/pdf/Armstrong_2001_Checklist.pdf (last accessed on 20 December 2019). Armstrong S and Green K, 'Forecasting methods and principles: Evidence based checklists' (2018), Journal of Global Scholars of Marketing Science. 28, 2. Available at https://www.tandfonline.com/doi/full/10.1080/21639159.2018.1441735 (last accessed on 20 December 2019).

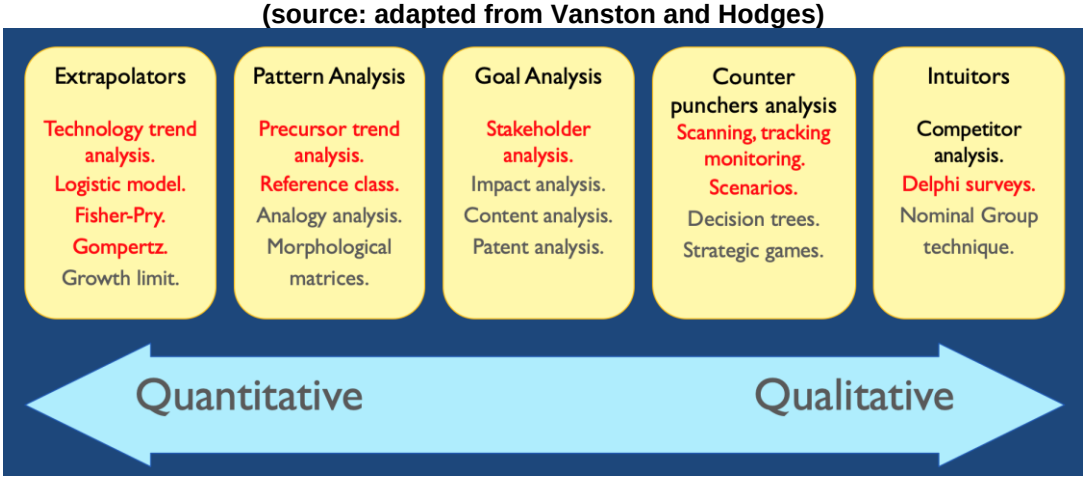
[627] https://www.cmu.edu/news/stories (last accessed on 20 December 2019).

6.5.1.1. Forecasting methods

To address common forecasting problems[628] this Study adopted a multiple methodological approach. Multi-methodology research combines qualitative and quantitative data, methods, methodologies, and/or paradigms for forecasting.

Academic research has highlighted that mono-method research can be improved through the use of multiple data, methods, methodologies, perspectives, standpoints, and paradigms.[629] This Study has therefore used a number of the quantitative and qualitative forecasting methods that are available to forecasters. The ten methods used in this Study are highlighted in red in Figure 9.

Figure 9 - Quantitative and qualitative forecasting methods (source: adapted from Vanston and Hodges)



Vanston and Hodge use their five views of the future methodology[630] as an extensive method for technology forecasting (see Figure 9). The five viewpoints on the future are the Extrapolator, the Pattern Analyst, the Goal Setter, the Counter-Puncher, and the Intuitor. They argue that an appreciation of all five views is most likely to produce good forecasts, good communication, and good decisions. The extrapolator and pattern analysis views, exemplified by substitution and adoption models, are the most suitable for developing quantitative results. Goal analysis, as the names suggests, adopts more qualitative analytical methods. Counter puncher methods are predictive methods that break forecasts into constituent elements. Intuitor analysis methods are based on structured communication and discussion.

A brief description of the quantitative and qualitative methods used by this Study (shaded in red in Figure 9) are provided below:

- *Technology Trend Analysis* – The practice of collecting information and attempting to spot a pattern, or trend, in the information.[631] This was achieved through desk research;

[628] Spyros Makridakis and Steven Wheelwright , 'Forecasting: Issues and challenges for marketing management' (1977), Journal of Marketing. Problems include technical difficulties, behavioural problems and organisational roadblocks. Available at https://www.researchgate.net/profile/Spyros_Makridakis/publication/270458049_Forecasting_Issues_Challenges_for_Marketing_Management/links/54be3bde0cf218d4a16a5590/Forecasting-Issues-Challenges-for-Marketing-Management.pdf (last accessed on 20 December 2019).
[629] Robert Burke Johnson and Larry Christensen, 'Quantitative, Qualitative, and Mixed Research Approaches' (2014), Sage, p.427 – 448.
[630] Lawrence Vanston and Ray Hodges, Technology forecasting for telecommunications (2004), available at www.tfi.com/pubs/w/pdf/telektronikk_peer.pdf (last accessed on 20 December 2019).
[631] WebFinance Inc, Trend analysis definition (2005).

- *Logistic Models* - A type of probabilistic statistical classification model. The logistic function develops an 'S-shaped' (sigmoid) curve.[632] This was undertaken during the development baseline models;
- *Fisher-Pry* – A technology substitution model based on assumptions about substitution and replacement caused by the advantages of new technology.[633] This was undertaken during the development baseline models;
- *Gompertz* - A technology substitution model based on assumptions about the deterioration of preceding devices, creating an 'S-shaped' curve that rises more steeply than other methods.[634] This was undertaken during the development baseline models;
- *Precursor Trend Analysis* – Precursor analysis improves upon trend analysis by using the forecaster's knowledge of factors that lead or cause trends.[635] This was achieved through desk research identifying catalysts and barriers and seeking expert input from our team and others;
- *Reference Class forecasting* – Based on theories of decision making under uncertainty this approach promises greater accuracy by taking an 'outside view'.[636] Comparisons of blockchain forecasts with previous technologies provided reference points for comparison with blockchain;
- *Stakeholder analysis* – Involves identifying the individuals or groups most likely to be affected by technology and assessing how their interests should be examined and addressed.[637] This was undertaken through engagement with experts using a blockchain briefing paper to encourage stakeholder input;
- *Scanning, tracking and monitoring* – Information is collected from many different sources to explore major trends, issues, advancements, events and ideas across a wide range of technological activities.[638] This was achieved through desk research presented in this chapter;
- *Scenarios* – A strategic planning method that is an adaptation and generalisation of classic methods used by military intelligence.[639] Engagement with experts using three scenarios (blockchain markets, smart contracts and utility tokens) in a briefing paper was used to encourage stakeholder input;
- *Delphi Surveys* – An interactive forecasting method that relies on structured communication with a panel of experts.[640] This was achieved through sharing blockchain forecasts to 2030 with experts during the Study and at the workshop.

Quantitative methods (technology trend analysis, logistic models, Fisher-Pry, Gompertz, precursor trend analysis) were used to develop a range of 'S-shaped' adoption curves for the adoption of key technologies that have been carefully monitored by Eurostat for more than 30 years.

[632] David Freedman, 'Statistical Models: Theory and Practice' (2009), Cambridge University Press.
[633] Fisher JC and Pry R, 'A simple substitution model for technological change'(1971), Technological forecasting and social change, 3, p.75-88.
[634] Porter I, Cunningham S, Banks J, Roper T, Mason T and Rossini F, 'Forecasting and management of technology' (1991), John Wiles and Sons, p138-145.
[635] US Department of Commerce, 'US Spectrum management policy: Agenda for the future' (1998), NTIA Special Publication 91-23.
[636] Blent Flyvbjerg, 'From Nobel Prize to Project Management: Getting Risks Right', Project Management Journal (2006), vol. 37, n°3, p.5-15, available at http://arxiv.org/abs/1302.3642 (last accessed on 20 December 2019).
[637] Weaver P, A Simple View of Complexity in Project Management (2007), Proceedings of the 4th World Project Management Week, Singapore.
[638] Patrick Dixon , 'Futurewise: The Six Faces of Global Change' (2007), Profile Books.
[639] Robert Barner, 'Team Troubleshooter: How to Find and Fix Team Problems' (2000), Davies-Black.
[640] Paul Foley and Masser I, 'Expert opinion and urban analysis Urban Studies (1987), 24, p.217 – 225.

These known and robustly documented adoption trends provide the basis for the reference class forecasting method that helps to underpin this Study. 'S-shaped' adoption curves, utilising input from stakeholders, have been formulated for blockchain market growth and the use of smart contracts. The results of reference class forecasting have then been shared and refined through the use of qualitative methods (stakeholder analysis, scanning tracking and monitoring, scenarios and Delphi surveys) with industry experts, business organisations, academics and other stakeholders online, during the project workshop and at other points in the Study.

6.5.1.2. Reference Class Forecasting

Reference class forecasting[641] is based on theories of decision making under uncertainty that won Princeton psychologist Daniel Kahneman the Nobel prize in Economics in 2002. Reference class forecasting promises more accuracy in forecasts by taking a so-called 'outside view' on prospects being forecasted, while conventional forecasting takes an inside view. The outside view on a given project is based on knowledge about actual performance in a reference class of comparable projects.[642]

The approach helps to overcome inaccuracy caused by optimism bias (judging future events in too positive manner) and political bias (over-estimation to increase personal benefits or approval. In essence, Reference Class Forecasting helps to overcome the excesses identified by the Hype Curve; described in the next section.

As noted above, 'S-shaped' adoption curves (using technology trend analysis, logistic models, Fisher-Pry, Gompertz) have been formulated for technology that has been monitored by Eurostat. These known and robustly documented adoption trends provide the basis for the reference class forecasting method that lies at the heart of this Study.

It is important to highlight that reference class forecasting examines previous technology adoption. These adoption rates for previous technologies will have been affected by the economic and social circumstances prevalent in each EU Member State. The importance or causality of characteristics such as gender, age, social status cannot be determined, but they are integrally incorporated in the 'S-shaped' curves developed for each technology, device or service.

'S-shaped' adoption curves can be observed for five technologies for which reliable Eurostat data is available (see Figure 10). The five technologies provide robust reference points for the rate of adoption in all 28 Member States and in individual Member States.

The five technologies emphasise two important issues relevant to this Study. Firstly, the speed of adoption varies (this is shown by the steepness of the curve). Slowest rates of adoption arise for computers, the fastest adoption rate has been observed for smartphones.

Secondly, tentative observations can be made about the differences in rates of adoption for two pairs of technologies – cell phones and their more functional successors smartphones (green lines in the figure), household internet adoption and the second-generation broadband internet (red lines in the figure). For both technologies, second 'round' technologies have been more rapidly adopted than their original first 'round'

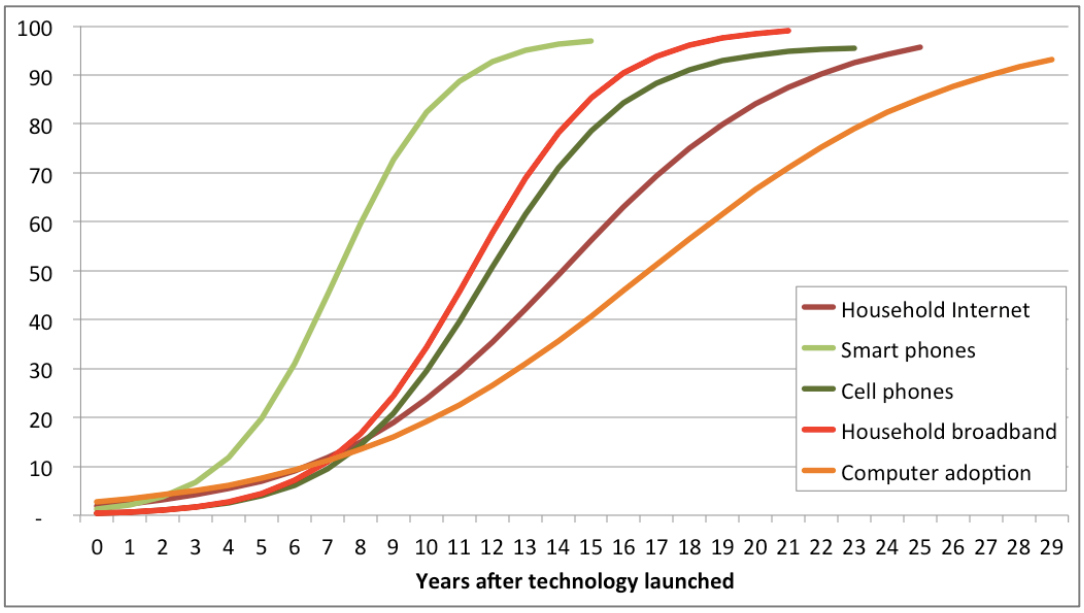
[641] Bent Flyvbjerg, Mette Skamris Holm, and Søren Buhl, 'Underestimating Costs in Public Works Projects: Error or Lie?'(2002), Journal of the American Planning Association, vol. 68, n°3, p.279-295.
[642] Bent Flyvbjerg, 'From Nobel Prize to Project Management: Getting Risks Right', Project Management Journal. Vol. 37, n° 3, p.5-15, available at http://arxiv.org/abs/1302.3642 (last accessed on 20 December 2019).

predecessors. It is also notable that more expensive items such as computers and household internet (which was considerably more expensive in 'real' terms than the subsequent broadband connections) are adopted less rapidly than other relatively cheaper technologies.

It is also arguable that what also drives second 'round' technology adoption is building upon first 'round' usage. For example, it can be argued that many smartphone buyers previously had featurephones and sought the extra functionality associated with a smartphone.

Section 6.1 highlighted that blockchain is different to most previous technologies, which were purchased by a citizen, business or other entity and used by them for social or economic advantage. In this respect, it is a new unknown technology and, as noted above, this type of technology previously has slow adoption rates. Conversely, it is a technology that will generally be utilised by users at little or no cost and this could enhance adoption rates.[643]

Figure 10 - EU adjusted S-shaped curves for five technologies (source: Tech4i2)

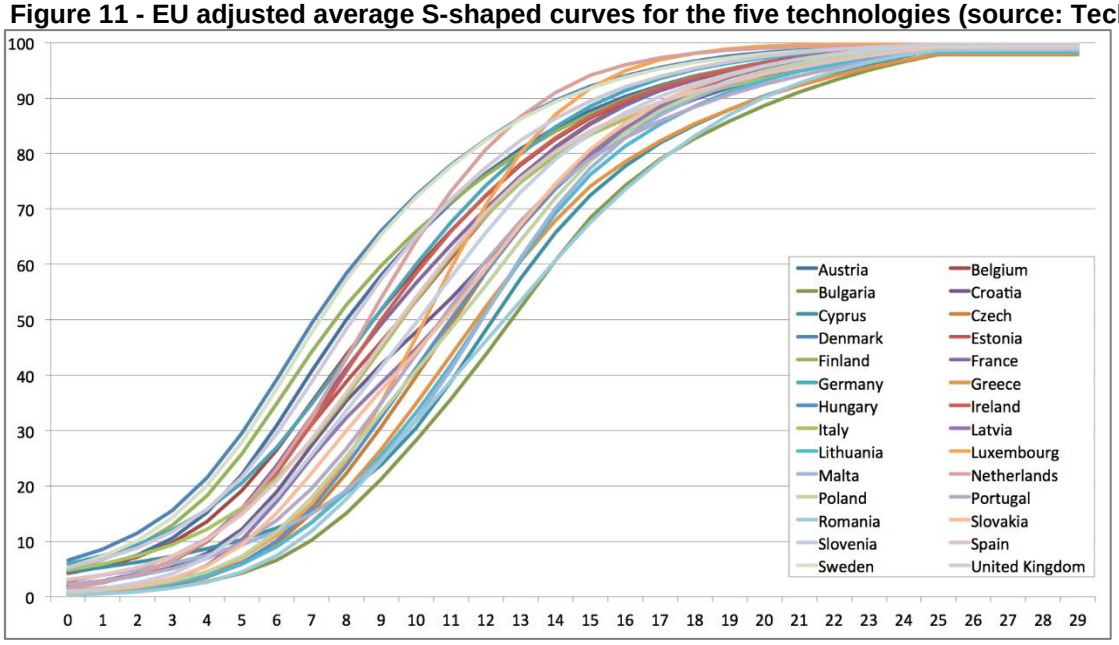


It is also important to highlight that the rates of adoption vary considerably between the 28 EU Member States. Countries with higher levels of GDP per capita generally adopt technologies faster than those with lower GDP per capita.

Whilst acknowledging this general wealth related principle, it is evident that there is considerable diversity in adoption patterns between Member States (see Figure 11, which provides adoption curves for the five technologies (in Figure 10) across the 28 EU Member States. For example, there is a five-year difference between the first Member States to reach 40 per cent adoption levels and the last. This difference increases to 6.5 years difference between the fastest and slowest Member States to reach the 80 per cent adoption level.

[643] Obviously a business or organisation will incur significant costs in developing and deploying blockchain for users.

Figure 11 - EU adjusted average S-shaped curves for the five technologies (source: Tech4i2)



6.5.2. Forecasting and the hype cycle

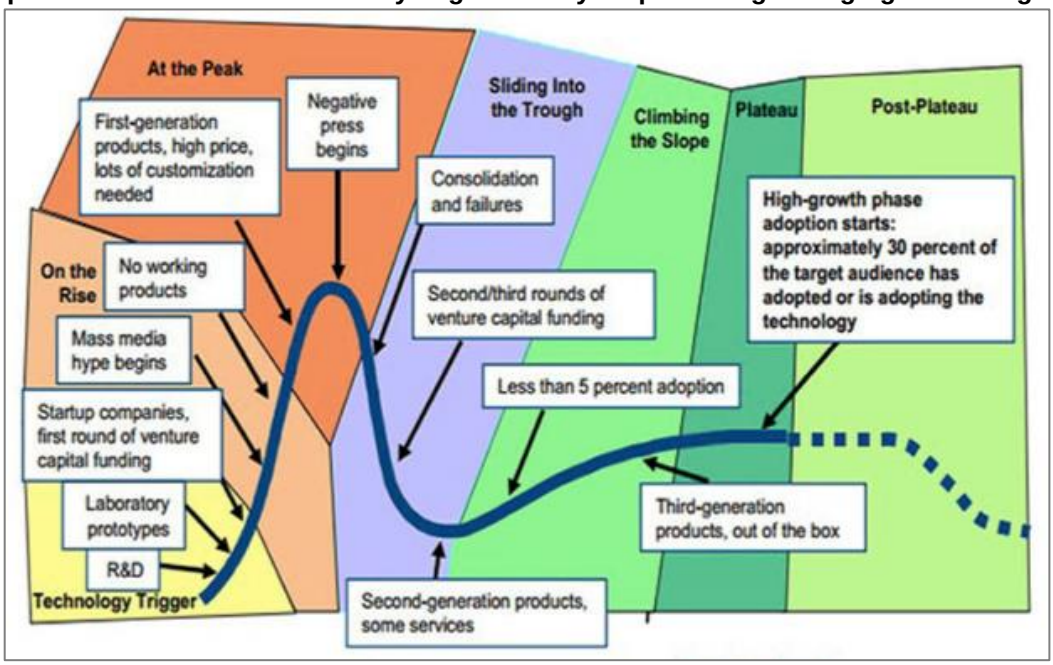
This Study, like any technology forecasting exercise, is based on predictions about technology postulated by consultants, academics, experts and other stakeholders in written reports and during engagement activities. It is therefore worth providing a cautionary note about the 'hype' that is sometimes associated with new technologies.

Charles McLellan undertook an interesting review of forecaster's reviews about emerging technologies. McLellan's study[644] highlighted the impact of the *Hype Cycle*, which is in fact not a cycle, it is more of a model of how technology gets promoted and then dismissed by commentators. The Hype Cycle plots a technology's typical progress from a Technology Trigger, through a period of increasing visibility to a Peak of Inflated Expectations, where negative coverage based on first-generation products precipitates a slide into the Trough of Disillusionment (see Figure 9). This is followed by a slower recovery, on the back of second-generation and subsequent products, up the Slope of Enlightenment to the Plateau of Productivity, where at least 30 per cent of the technology's target audience has adopted the technology.

McLellan examined emerging technologies flagged by Gartner between 2003 and 2014 — a 12-year period encompassing a great deal of economic and technological change to examine the technologies that made it to maturity, and those that were stillborn or still gestating (see Figure 12). The position of a technology on the Hype Cycle reflects the collective judgement of Gartner's analysts, rather than the analysis of specific data. Although, of course, a vast amount of research data informs analysts' judgements.

[644] Charles McLellan, 'Analysing the analysts: Predicting emerging technologies' (2014), http://www.zdnet.com/article/analysing-the-analysts-predicting-emerging-technologies (last accessed on 20 December 2019).

Figure 12 - Market events during the technology Hype Cycle (source: McLellan http://www.zdnet.com/article/analysing-the-analysts-predicting-emerging-technologies)

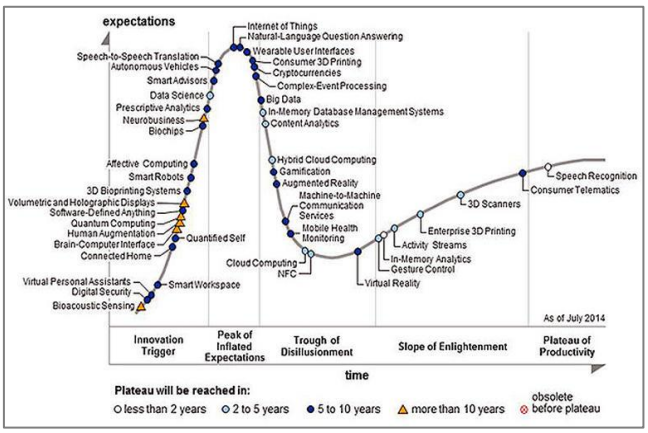


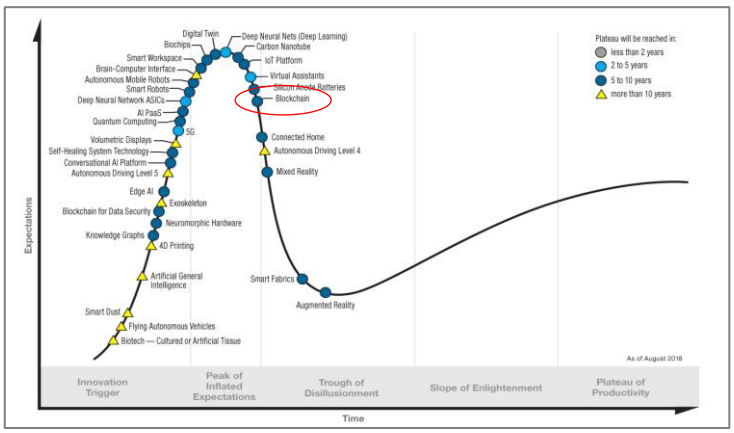
McLellan looked back over 12 years' worth of Hype Cycles for Emerging Technologies, logging entries for 192 different technologies mentioned between 2003 and 2014. Some, such as cloud computing and big data, are now well known and widely implemented. Others, like folksonomies and neurobusiness probably remain unfamiliar to many people.

Out of the 192 emerging technologies flagged by Gartner between 2003 and 2014, just 11 (5.7 per cent) had reached the Plateau of Productivity, while 28 (14.6 per cent) had made it to the Slope of Enlightenment by 2014. 79.7 per cent had failed to progress beyond the Technology Trigger (24.5 per cent), Peak of Inflated Expectations (24 per cent) or Trough of Disillusionment (31.2 per cent) stages. Of course, hype cycles include recent technologies that may well mature in future, so to get a more representative picture McLellan looked at those first mentioned between 2003 and 2008 (the first 6 of the 12 years examined). As might be expected, by 2014 a bigger percentage had made it to the Plateau of Productivity (7.4 per cent) and a smaller proportion had failed to progress beyond the Technology Trigger (20.4 per cent). 37 per cent remained mired in the Trough of Disillusionment.

The technology Hype Cycle provides a cautionary note about predicting the development and adoption of new technologies. Indeed, it is interesting contrasting the 2014 hype cycle with the 2019 edition five years later (see Figure 13). Blockchain did not appear in 2014, but in 2019 it featured, and was quite advanced in its path (just entering the trough of disillusionment), whilst others such as quantum computing and autonomous driving had remained largely static.

Figure 13 - The 2014 and 2019 Gartner Hype Cycles for Emerging Technologies





6.5.3. Blockchain forecasts

Using the preceding methodologies, research developed forecasts for the three key foci for this Study: blockchain market growth, the use of smart contracts in intra-EU28 trade and utility tokens. The goal of the research was to develop baseline models of the likely adoption/utilisation trends for the key foci between 2019 and 2030. The baseline model is a meta-analysis best estimate of the future.

As the Carnegie Mellon highlighted in Section 6.5.1 "a forecast is never 100 per cent accurate". But the baseline model will provide a common logical basis against which to estimate the impact of the policy options developed by this Study.

Desk research was used to find qualitative and quantitative studies that provided information about forecasts and/or trends. This research found more than 100 studies and papers. Many of these are referenced in footnotes. Where studies were thought to be too obtuse[645] or predictions were too far from the average across other studies; they were omitted.

Clearly, 'selecting the best forecast' is an oxymoron. No one can know the best forecast until the date of the forecast has been reached and, ex post, the closest forecast to the item being studied can be identified.

In this ex ante research, studies from well-known and more prestigious organisations were given prominence, as were those that provided similar values to the mean and median values of forecasts across all the studies providing suitable data. These average insights from multiple studies where available were then developed into scenarios and 'S-shaped' adoption curves.

Stakeholder engagement concerning these forecasts was sought using Delphi methods. Two rounds of consultation were undertaken.

The first round of Delphi analysis received replies from nearly 30 of the 200 experts contacted by email.[646] Their qualitative and quantitative views were sought using a four-page briefing document, which provided insight to relevant forecasts and scenarios that had been developed (see Annex V). A short questionnaire on the final page of the briefing asked four qualitative questions about barriers and catalysts for development

[645] Some forecasts appeared to lack intellect and robustness, others seemed erroneous.
[646] The contacted experts included industry representatives, entrepreneurs, policy makers, economists, lawyers and other stakeholder groups. A very similar mailing list was used to invite workshop participants. Replies were received from all of these groups.

and seven quantitative questions about reader's views on the validity of forecasts found from secondary sources.

Feedback from experts who contributed to the first round of Delphi consultation was shared at a workshop hosted in cooperation between the Commission and the Consortium.[647] Those attending were asked to provide their views in a second round of Delphi consultation.[648] In both exercises, some voiced concern that they found the exercise difficult or beyond their immediate expertise. Nonetheless just over 40 replies at the workshop were received and these results were sued to further refine forecasts.

Critical insights were provided during expert engagement about four key issues required to develop 'S-shaped' adoption curves for technology:

- When will the technology begin to be adopted?
- What will be the rate of adoption?
- How long until market saturation is reached?
- What is likely to be the maximum market size and/or will the technology be successful?

Forecasts about all of the above issues were provided in the briefing paper, contributors merely had to voice their opinion on the validity of forecasts. The briefing document and questions are provided in Annex V.

The remainder of this section focuses on the development of the baseline models. Three models, which will form the basis for testing policy options, are presented in this section. The next section provides insights to general growth patterns for blockchain.

6.5.3.1. Blockchain impacts

A number of organisations have made forecasts about growth in blockchain market expenditure and growth in blockchain enabled transactions. Research has standardised these forecasts to expenditure or impact in 28 EU Member States in euros between 2019 and 2030. For example, a Critical Future report suggests global blockchain market expenditure will grow by 62.6 per cent per annum (CAGR), reaching €9.3 billion in 2024. The 28 EU Member States import 21.1 per cent of world trade in services.[649] If this figure is used as a probably conservative measure of EU28 blockchain investment, it suggests a blockchain market size of €1.96 billion in 2024. Section 6.4.2 noted that investment in EU28 blockchain start-ups comprised 22 per cent of global investment. Adoption of a figure of 21.1 per cent therefore does not seem unreasonable.

[647] The range of responses provided by first round respondents were shared with all those attending the workshop. The responses from the first round of Delphi were presented in exactly the same manner as those presented in Figure 14, Figure 16, Figure 18, Figure 20 (these figures provide aggregate results after two rounds of Delphi). Alignment between the first and second Delphi rounds was broadly similar.
[648] The email list of approximately 200 people used to invite people to the workshop was used to make contact with participants in the first round of the Delphi study. The experts on the list included industry representatives, entrepreneurs, policy makers, economists, lawyers and other stakeholder groups. Throughout the Delphi study and the workshop, experts could self-exclude if they felt they lacked confidence in their forecasts. Debates about who (or in the context of this Study which groups) can best predict the future have a long history. Also see: Epstein, The peculiar blindness of experts (2019), available at: https://www.theatlantic.com/magazine/archive/2019/06/how-to-predict-the-future/588040/.
[649] Op.cit, Eurostat, The EU in the world: International trade (2018).

Our Study sought the views of Delphi participants and workshop attendees[650] about the forecast and about the timespan for adoption when market saturation would be achieved.

Figure 14 - Expert views using the Delphi methodology about the accuracy of the Critical Futures market expenditure forecast of €1.96 billion in EU28 in 2024

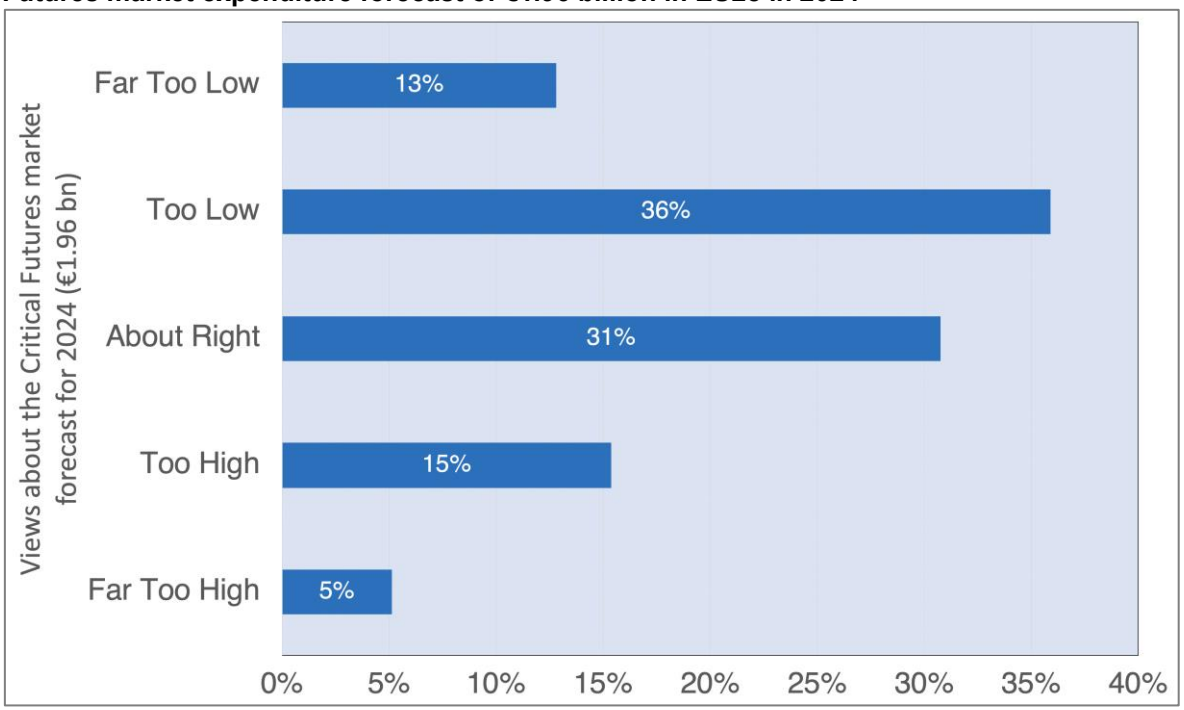


Figure 14 shows that nearly one third (31 per cent) of respondents thought the forecast was about right. Nearly half (49 per cent) thought that it was too low (or far too low) and 20 per cent thought that the forecast was too high (or far too high).

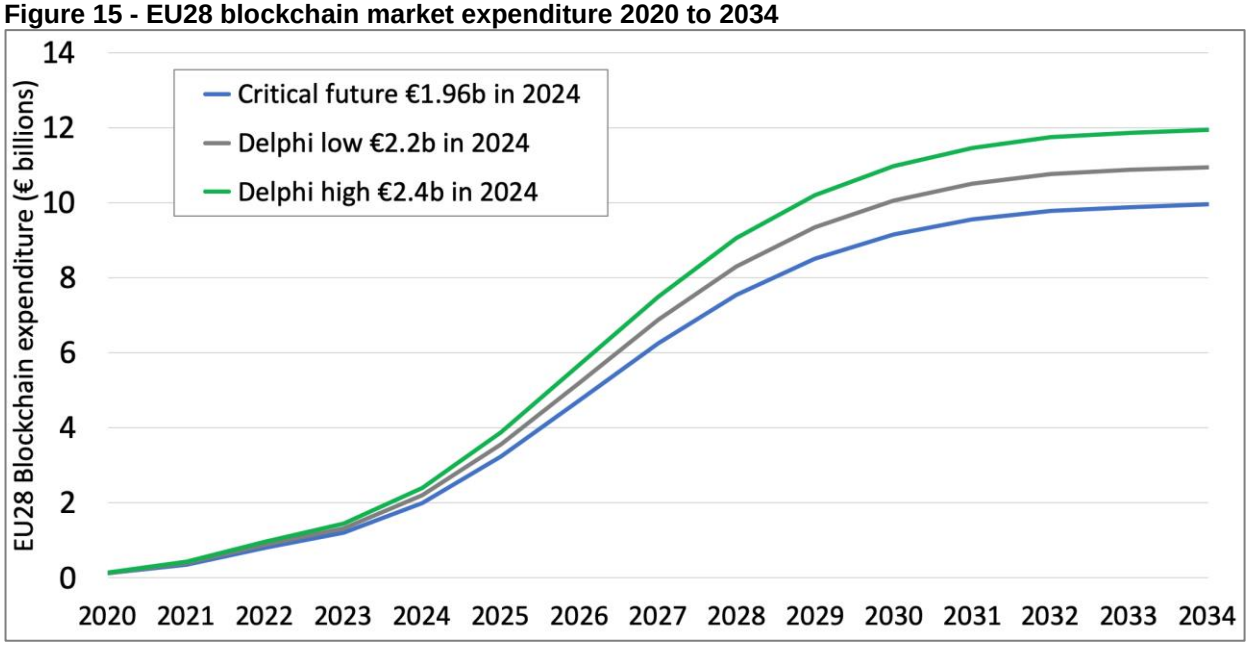
The average year when market saturation was estimated to occur was 2034. The preceding review of the timespan for the adoption of five technologies in the 28 EU Member States (see Figure 10) highlights that this would be a relatively fast rate of adoption - 14 years to reach market saturation has only been achieved by the smart phone, the four other technologies have been slower.

Using feedback from the two rounds of Delphi surveys it was possible using 'S-shaped' adoption methodologies to create forecasts for the blockchain expenditure in the 28 EU Member States up to 2034 (see Figure 15). The graphic presents the Critical Future forecast of €1.96 billion per annum in 2024 in the blue line. Figure 14 highlighted that the majority of respondents thought this figure was too low. The grey line therefore represents a ten per cent increase in the Critical Future 2024 forecast.[651] The green line provides a forecast to demonstrate a 20 per cent increase in the 2024 forecast.

[650] In essence two rounds of Delphi surveys were undertaken, emails received responses from almost 30 experts, just over 40 people responded at the workshop. Not all participants answered all elven questions in the questionnaire.

[651] Annex V highlights that as well as using a Lickert scale for answers, respondents were also invited to provide their own precise forecast for the size of the global blockchain market in 2024. Analysis of these insights led to the adoption of ten and 20 per cent increases in the Critical Forecasts since these value best reflect the relatively small increases predicted by most respondents.

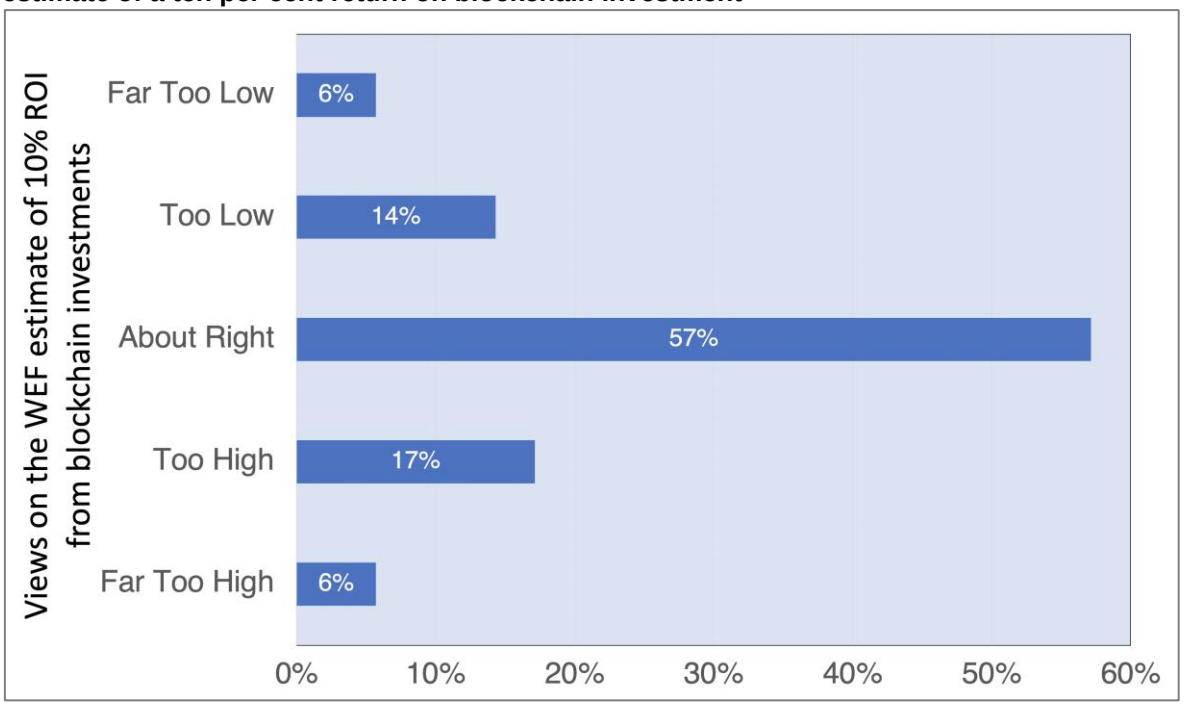
Figure 15 - EU28 blockchain market expenditure 2020 to 2034



Investment data is only useful when considering impacts if rates of return on blockchain investment are known.[652] The World Economic Forum (WEF) undertook an interesting global blockchain survey of 550 individuals across 13 industries, including interviews with public-sector leaders and private-sector chief executive officers.[653] The study found that on average respondents expected a 24 per cent return on investment on blockchain projects, but after projects were completed, they only realised only a 10 per cent return. The Delphi study investigated the views of experts about the accuracy of a 10 per cent rate of return. Figure 16 shows a remarkable degree of convergence in expert views.

[652] It is important to highlight that in this context a return is not simply an increase in output. Returns can also include other financial and competitive advantages such as efficiency improvements or enhanced service quality.
[653] World Economic Forum, 'Building value with blockchain technology: How to evaluate blockchains benefits' (2019), available at http://www3.weforum.org/docs/WEF_Building_Value_with_Blockchain.pdf (last accessed 20 December 2019) .

Figure 16 - Expert views using the Delphi methodology about the accuracy of the WEF study estimate of a ten per cent return on blockchain investment



Prior to embarking on a blockchain project, 59 per cent of respondents stated they had no confidence that the project would deliver a positive return on investment – and only 38 per cent of those who have implemented the technology developed a business case prior to investing. Many of those interviewed had doubts as to whether the technology was production-ready – 'limitations on blockchain technology' and 'scalability issues' were selected as the biggest challenges in adopting blockchain. If the 10 per cent return on investment figure from the WEF study is adopted the forecast returns of €1 billion to €1.2 billion in 2034. The same study highlights that these benefits will probably be lagged by one to four years after investment.

Further insights about blockchain impacts can be found from studies examining the impact of blockchain on trade. The Centre for Economics and Business Research undertook research, including insights from 247 global contract and commercial managers, to examine how reducing trade frictions using blockchain technologies would impact on global trade.[654] The study utilised an econometric approach to global trade flow data on a volume and value basis, looking specifically at goods trade. The econometric model assumed a 2.5 per cent reduction in costs due to the utilisation of smart ledger technologies and utilised container import and export cost figures obtained from the World Bank. Analysis estimated that the removal of 2.5 per cent from transport costs would represent a yearly global trade value of €32.2 billion. In 2016, the 28 EU Member States had 16.2 per cent of global exports. Using this percentage (16.2 per cent) one can estimate an EU28 figure from the impact of blockchain on global trade (at 2.5 per cent). This calculation suggests annual trade benefits of €5.2 billion.[655] Whilst this study is interesting is does not provide robust information about the source of the

[654] Douglas McWilliams , Cristian Marcu and Beatriz Cruz, 'The economic impact of smart ledgers on world trade'(2018), available at https://www.longfinance.net/media/documents/Economic_Impact_Of_Smart_Ledgers_On_World_Trade.pdf (last accessed on 20 December 2019).

[655] Eurostat, 'The EU in the world: International trade' (2018), available at https://ec.europa.eu/eurostat/statistics-explained/pdfscache/20442.pdf (last accessed on 20 December 2019).

figure of '2.5 per cent' for savings, nor a time span over which the benefit might accrue. More thorough studies examining the impact on trade have generally focused on benefits from smart contracts. These are considered in the next section.

6.5.4. Smart contracts

Two particular areas of attention have been identified for this Study; smart contracts and utility tokens. The workshop highlighted that even in these two seemingly well-defined areas considerable variation can exist. This section reviews forecasts and impact studies concerned with smart contracts. The next section considers utility tokens.

Smart contracts have been defined as 'automated software agents hosted on blockchains that are capable of autonomously executing transactions when certain conditions arise'.[656] Although smart contracts are not necessarily smart (they only carry out what they are programmed to do) nor contracts, they can be used in contractual settings.[657]

In trustless public blockchain networks, smart contracts are simply computer programs consistently executed by a network of nodes, without the arbitration of a trusted authority'.[658] The utilisation of smart contracts can have legal implications, particularly regarding enforceability, these were investigated further in the previous chapters.

Deloitte reported paper systems drove US$18 trillion in global transactions per year in 2014 and smart contracts offer considerable opportunities to decrease costs and improve reliability.[659]

World Trade Organisation source data[660] for 2014, used by Deloitte, does not reveal the volume of transactions between the 28 EU Member States and the rest of the world nor intra-EU trade. However, Eurostat provides details for both of these transactions.[661] Since this Study focuses on the 28 EU Member States, intra-EU trade was investigated. These transactions were selected because they represent the geographical area over which the European Union has jurisdiction. Intra-EU trade (rather than trade within a single Member State) was selected because this is the tier at which EU jurisdiction will have the greatest benefit. Subsidiarity and proportionality principles authorise intervention by the Union when the objectives of an action cannot be sufficiently achieved by the Member States, but can be better achieved at Union level, 'by reason of the scale and effects of the proposed action'. It was therefore considered erroneous to examine trade within in a single Member State because legislation and regulations could be established by the government of that country.

---

[656] Jake Goldenfein and Andrea Leiter, 'Legal Engineering on the Blockchain: "Smart Contracts" as Legal Conduct' (2018) Law and Critique (Forthcoming). Available at SSRN: https://ssrn.com/abstract=3176363 (last accessed on 20 December 2019).

[657] Nick Szabo, 'Smart Contracts: Building Blocks for Digital Markets', EXTROPY: The Journal of Humanist Thought (1996), . available at http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (last accessed on 20 December 2019), p.16.

[658] Massimo Bartoletti and Livio Pompianu, 'An empirical analysis of smart contracts: Platforms, applications, and design patterns' (2017), in *Michael Brenner et al (eds), Financial Cryptography and Data Security*, Springer. Available at https://www.springerprofessional.de/en/an-empirical-analysis-of-smart-contracts-platforms-applications-/15236404 (last accessed on 20 December 2019).

[659] Deloitte, 'CFO Insights: Getting smart about smart contracts' (2016), available at https://www2.deloitte.com/tr/en/pages/finance/articles/cfo-insights-getting-smart-contracts.html (last accessed on 20 December 2019).

[660] WTO, International Trade Statistics (2015), available at https://www.wto.org/english/res_e/statis_e/its2015_e/its2015_e.pdf (last accessed on 20 December 2019). An exchange rate of 0.73 was used to convert US$ values into euros for 2014.

[661] Eurostat, "Intra-EU28 trade, by Member State, total product" (2019), https://ec.europa.eu/eurostat/databrowser/view/tet00047/default/table?lang=en (last accessed on 20 December 2019).

The value of trade in goods between the 28 EU Member States in 2014 was €2.9 trillion and Eurostat estimated this had risen to €3.3 trillion in 2018. Whilst the volume of trade within the 28 EU Member States provides interesting insights of the total market size that smart contracts might be able to transform, it does not provide an insight to the number of contracts (smart or otherwise) that might be generated. To enable this calculation, it is necessary to understand the average value of an intra-EU trade transaction. Friederike and Scmidt-Eisenlohr[662] provide an estimate for each transaction in the US for 2010 to 2012, this equates to €34,160.

Through linear extrapolation we estimate that by 2018, this average figure will have risen to approximately €40,750.[663] If this figure is adopted it suggests that the number of transactions supporting intra-EU trade between the 28 EU Member States would be 84 million in 2019.

Figure 17 presents the preceding information in a graphical format. The blue bars provide linear extrapolation forecasts from Eurostat data, for the value of intra-EU trade in billions of euros (using the vertical axis on the left). The black line forecasts the number of transactions supporting intra-EU trade between the 28 EU Member States, this is measured by the vertical axis on the right. There are forecast to be 84 million in 2019 and 107 million in 2030.

The green line presents the Delphi study forecast of blockchain market saturation by 2034 to estimate the number of transactions that could be facilitated by blockchain.[664] This estimates 102 million blockchain supported transactions in 2030.

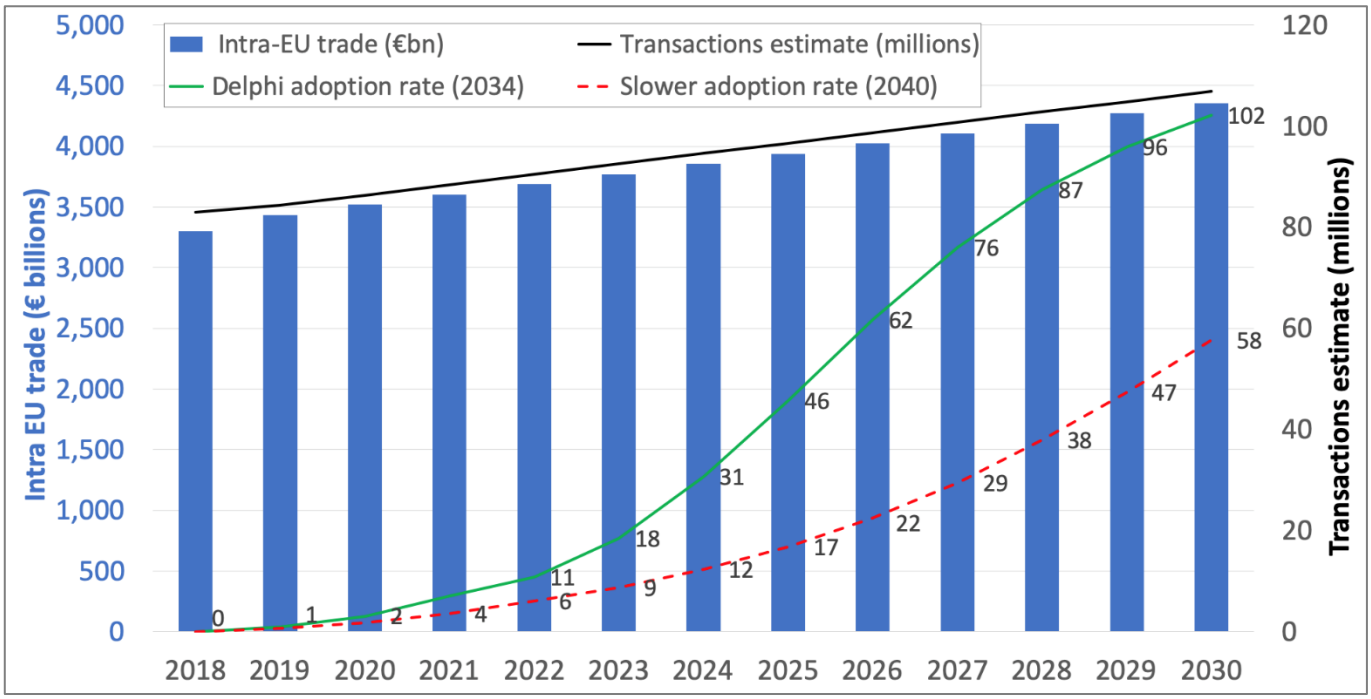
A red 'S-shaped' adoption line provides forecasts for the number of transactions if market saturation was achieved eight years later in 2042, this is a more conservative estimate. This forecast estimates the 58 million intra-EU transactions will be supported by blockchain in 2030. Using this slower adoption curve, the volume of transactions undertaken by smart contracts is just over half the total volume (54 per cent) in 2030.

[662] Niepmann Friederike and Tim Scmidt-Eisenlohr, 'International trade risk and the role of banks' (2015), International Finance Discussion Papers n° 1151, available at https://www.federalreserve.gov/econresdata/ifdp/2015/files/ifdp1151.pdf (last accessed on 20 December 2019), p22. An exchange conversion rate of 0.8 is used for 2010 to 2012. No similar European studies have been found.

[663] United States volume of merchandise trade exports was US$ 1,482 billion in 2011 (United Nations Conference on Trade and Development , Statistics database 2018, https://unctad.org/en/PublicationsLibrary/ditctab2019d2_en.pdf (last accessed on 20 December 2019). This would suggests that 34.7 million transactions took place. If one assumes that the number of transactions remains broadly similar but that the values of transactions might increase it is useful to examine the average value of 34.7 million transactions for the US$ 1,664 billion trade that took place in 2018. This calculation suggests an average value of US$ 47,900 or €40,750 using an average 2018 exchange rate of 0.85.

[664] Delphi study participants predicted market saturation in 2034 when market size was forecast to be €4,700 billion. The participants generally agreed with the Critical Future forecast of €1.96 billion per annum in 2024. Extrapolative methodologies were then used to match an s-shaped curve over a ten-year time period to these two points.

Figure 17 - Intra-EU trade, transactions and potential smart contract adoption 2018 to 2030



One of the few studies to provide evidence based quantitative insights to the economic impact at the micro (business) level was undertaken by Forrester for IBM in 2018.[665] Research examined projects costs savings, business benefits and the costs associated with introducing IBM's blockchain product in six businesses (two financial services businesses, a logistics company, a utilities business, a security and authentication company and a blockchain consulting company).[666] The study estimated that savings from blockchain smart contracts and data integration are €4.60 per transaction.[667]

The Delphi study investigated the views of experts about the Forrester estimate (see Figure 18). The majority of respondents (53 per cent) thought that the estimate of a €4.60 saving per blockchain facilitated transaction was 'about right'. A quarter (25 per cent) thought that the figure was 'too low'. Therefore, when estimating the total value of savings from utilising blockchain for intra-EU trade, the Forrester estimate of €4.60 is used together with a slightly higher value of €5.00 per transaction.

[665] Op.cit, IBM, 'Emerging Technology Projection: The Total Economic Impact Of IBM Blockchain: Projected Cost Savings And Business Benefits Enabled By IBM Blockchain'. (July 2018).
[666] A note of warning must be made about the fact that study was commissioned and published by IBM, it is unlikely companies not benefiting (or those receiving insufficient rewards) from blockchain implementation would be included in the analysis.
[667] This saving is simply for data integration. It is likely additional benefits would arise from decreases in other export related activities. It is acknowledged that this figure is derived from six use cases in different sectors. Differences could arise in different sectors and use cases. Until further studies are available this is thought to be the only study that provides insights.

Figure 18 - Expert views using the Delphi methodology about the accuracy of the Forrester estimate of a €4.60 saving per blockchain facilitated transaction

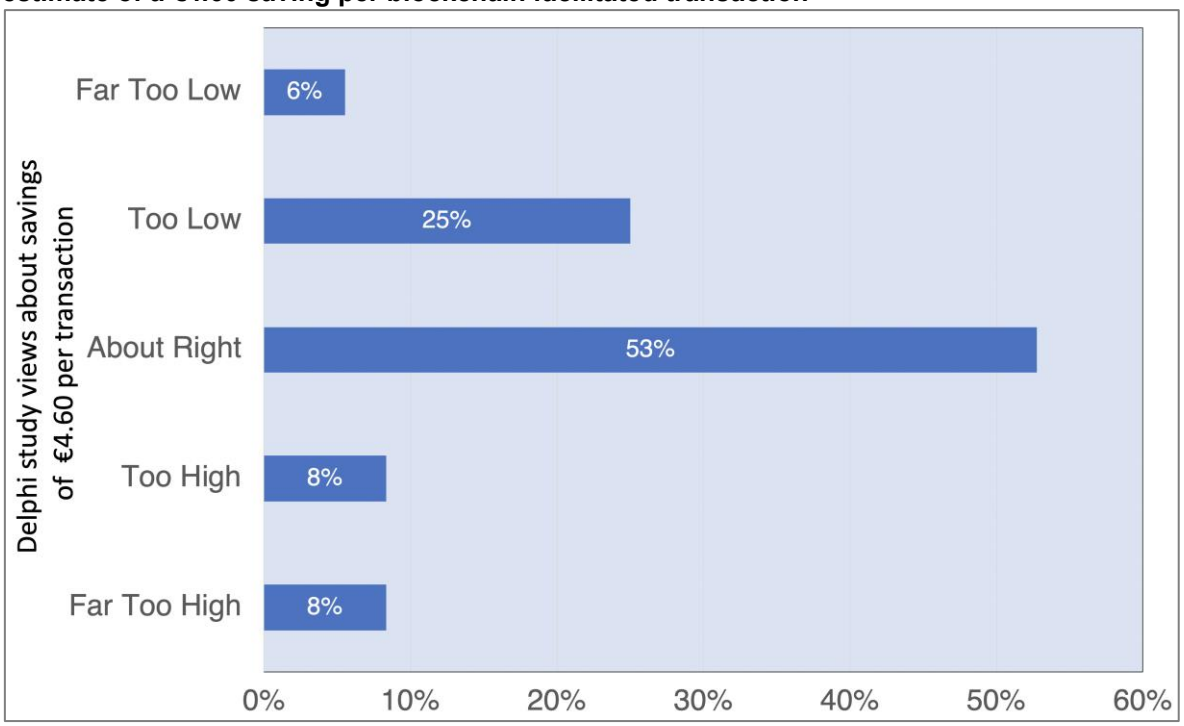
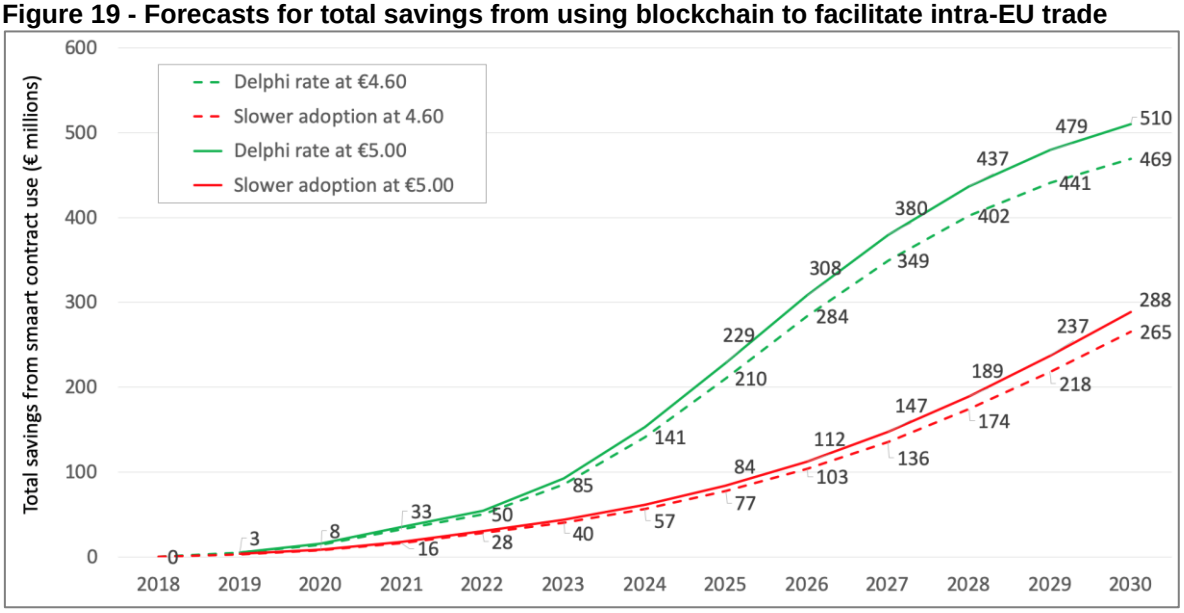


Figure 19 utilises the two values of €4.60 and €5.00 savings per transaction facilitated by blockchain to estimate the total value of savings from utilising blockchain for intra-EU trade.

The green lines utilise the Delphi study forecast of blockchain market saturation by 2034 to estimate savings at a rate of €4.60 and €5 per transaction. These forecasts suggest that total savings of between €469 and €510 million per annum could be from utilising blockchain for intra-EU trade in 2030. This figure would rise to maximum of €574 million when market saturation is reached in 2034. The cumulative size of these savings between 2019 and 2030 would be €2.5 billion at the lower rate and €2.7 billion if transaction savings are €5 per transaction.

Figure 19 - Forecasts for total savings from using blockchain to facilitate intra-EU trade



A red line provides forecasts for the number of transactions if market saturation was achieved eight years later in 2042. Due to a slower rate of adoption, total savings are smaller, ranging between €265 million and €288 million per annum in 2030. The cumulative size of savings at the lower rate of adoption between 2019 and 2030 would be €1.1 billion if savings are €4.60 per transaction and €1.2 billion at the higher rate.

In the first instance, these relatively significant benefits will arise for the buyers, sellers, logistics companies and other stakeholders in the supply chain.[668] However, it is likely that over time, some of these savings could be used to reduce the cost of goods for consumers. This is particularly likely to arise in competitive markets where price is a significant factor determining sales.

6.5.5. Tokenisation and cryptocurrencies

A final area of focus for this Study is tokenisation, particularly utility tokens. The European Securities and Market Authority (ESMA) and Member State securities authorities are currently investigating security tokens in a Task Force.

Tokenisation is the digital representation of a physical or intangible asset (e.g. IP rights and dematerialised securities held in a central securities depository account).[669] A token is a depiction of a particular asset or utility. There are three key types of tokens:

- *Currency tokens* - These are crypto currencies such as Bitcoin. Currency tokens are built on their own independent blockchains.[670] They are not based on assets, instead, their value is directly linked to the mechanism that distributes them.[671] Initial coin offerings (ICOs) usually limit the number of tokens and set a low price for each token;[672]

[668] 'Trickle down' impacts across other sectors will also arise if resources saved are reinvested in other ventures or sectors.
[669] Lauren Coleman, 'Here's why interest in tokenising assets is starting to surge' (2019), https://www.forbes.com/sites/laurencoleman/2019/04/25/heres-why-interest-in-tokenizing-assets-is-starting-to-surge/#63cacb3840a5 (last accessed on 20 December 2019).
[670] Stephen O'Neal, 'Tokenisation explained' (2019), https://cointelegraph.com/explained/tokenization-explained (last accessed on 20 December 2019).
[671] This value is usually associated to the utility derived by users.
[672] Some tokens have are not issued via and ICO.

- *Securities tokens* - These tokens are cryptographic tokens that pay dividends, share profits, pay interest or invest in other tokens or assets to generate profits for the token holders.[673] A cryptographic representation of an organisation's shares, bonds, property or other assets provides instant liquidity.[674] The European Securities and Markets Authority and the EU Member State securities authorities are currently examining the status of securities tokens;
- *Utility tokens* – These are digital assets used to finance or support a network by providing token holders with a guarantee of being able to consume some of the network's products or services.[675] Most of the current utility tokens are based on the Ethereum blockchain.[676] A similar example, though not currently on blockchain, is crowdfunding on KickStarter or GoFundMe where the buyer of a utility token has paid the issuer of the token money now so that the company can develop a product that the buyer of the token can later redeem for that good or service. Utility tokens differ from security tokens because they do not confer rights of ownership over an organisation or company.

Satoshi Nakamoto developed the first currency token - Bitcoin - in 2008.[677] Bitcoins are created by a mining process at a current rate of 1,88 Bitcoins every day (657,000 per year). The number of Bitcoins in circulation will be capped at 21 million, which is expected to be reached around 2140. The computing power requirements and energy consumption issues associated with this growth are examined in Section 6.5.6.4.

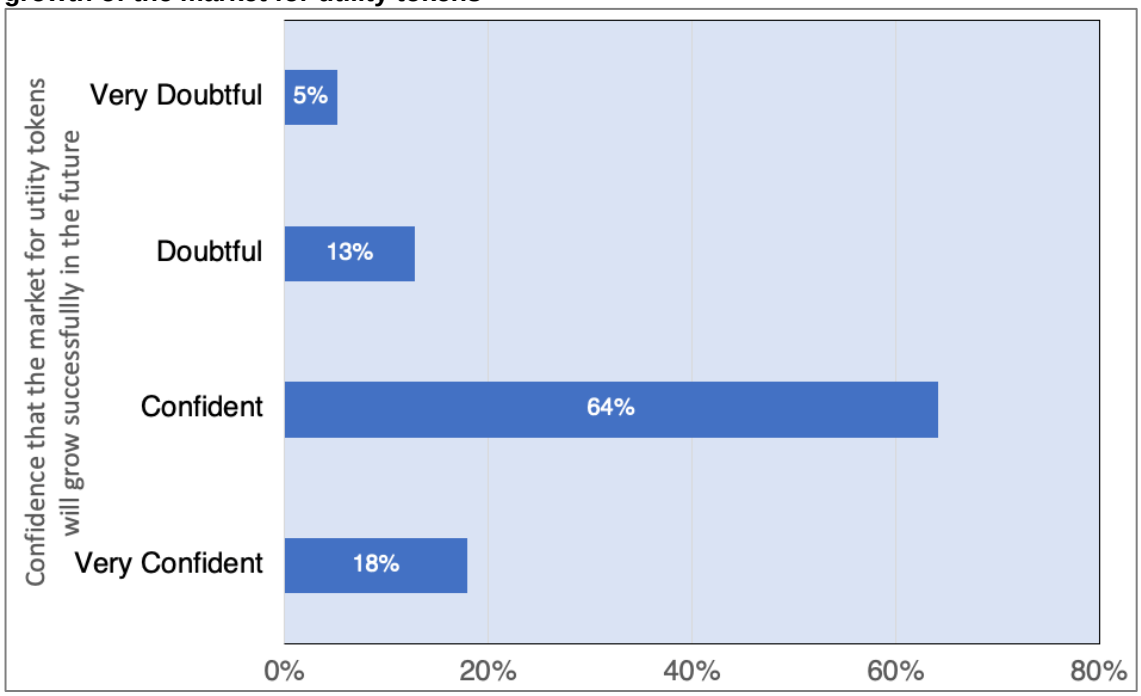
Other cryptocurrencies have been created. Litecoin is regarded as a rival to Bitcoin. It is designed for processing smaller transactions faster. Unlike the heavy computer horsepower required for Bitcoin mining, Litecoins can be mined by a normal desktop computer,[678] more recently miners use graphics cards and ASICs. Litecoin's maximum limit is 84 million – four times Bitcoin's 21-million limit – and it has a transaction processing time of about 2.5 minutes, about a quarter that of Bitcoin. MintChip was created by the Royal Canadian Mint. MintChip is a smartcard that holds electronic value, and which can be transferred from one chip to another. Like Bitcoin, MintChip does not need personal identification. Unlike Bitcoin, it is backed by a physical currency, the Canadian dollar.

Information about ICOs is available, but interest in the phenomenon has cooled considerably since the start of 2018. White and Case[679] report a large increase in initial coin offerings. In 2017 more than 850 global public ICOs raised over €5.3 billion for developers[680]. They forecast this global figure would increase to €17.6 billion in 2018.

[673] Christina Majaski, 'Security token definition' (2019), https://www.investopedia.com/terms/s/security-token.asp (last accessed on 20 December 2019).
[674] Agrawal H, 'What are security tokens and why is the market bullish' (2019), https://coinsutra.com/security-tokens/ (last accessed on 20 December 2019).
[675] Medium Corporation, 'Utility tokens: How they work and why they are so important' (2018), https://medium.com/coinbundle /utility-tokens-978d117290cd (last accessed on 20 December 2019).
[676] Joel Camacho, 'Utility tokens: A general understanding' (2018), https://medium.com/coinmonks/utility-tokens-a-general-understanding-f6a5f9699cc0 (last accessed on 20 December 2019).
[677] Northeastern University, 'Guide to the rise of cryptocurrency (2019)', https://onlinebusiness.northeastern.edu/neu-msf/guide-to-the-rise-of-cryptocurrency-digital-currency-and-Bitcoin/ (last accessed on 20 December 2019).
[678] Adam Barone 'The future of Cryptocurrency in 2019 and beyond' available at https://www.investopedia.com/articles/forex/091013/future-cryptocurrency.asp (last accessed on 20 December 2019). Reaching the capping limit in 2140 appears to be an error. Regardless of how many are already in existence 21 million will have been created between January 2019 and February 2035.
[679] White and Case, 'International ICOs – legal challenges and implications' (2018), https://www.whitecase.com/publications/alert/international-icos-legal-challenges-and-implications (last accessed on 20 December 2019).
[680] At a mid-year exchange rate of 0.88 in 2017.

The Delphi study investigated the views of experts about their confidence that the market for utility tokens would grow successfully in the future (see Figure 20). Nearly two thirds of respondents (64 per cent) were confident. Conversely, 18 per cent were either doubtful or very doubtful about prospects for success.

Figure 20 - Expert views using the Delphi methodology about confidence in the successful growth of the market for utility tokens[681]



6.5.6. Social benefits and impacts

Preceding sections have focused on the three key areas assigned for this Study. Some of the spin-off or indirect socio-economic benefits arising in these areas have been described. This section takes a closer look at social and environmental impacts and benefits. It also provides insights to some of the innovative ways that utility tokens might be used to provide social and environmental benefits.

The development of policy options and their impact are the primary focus for this Study. Economic analysis of policy impacts can be described in monetary terms, which are relatively easy to share and comprehend by most experts. Social and environmental benefits are equally important, but generally more amorphous, and thus harder to describe and comprehend. In the same manner as previous sections in this chapter, this section focuses on presenting the social and environmental forecasts that are most interesting and possibly reliable. As noted previously, no one can have detailed knowledge of what the future will hold. It is important that these benefits and impacts are also presented in this report. Expert stakeholders were not asked to comment on them during the Delphi survey or workshop.

A number of social benefits are forecast to arise from the utilisation of blockchain capabilities. Many benefits to society will also arise from the use of blockchain

[681] The development of utility tokens is at an early stage of development. Their applications could be considerable, but studies predicting growth across applications have not been found. Those attending the workshop noted this diversity and the need to monitor this area in the future. The next section, examining social and environmental benefits, provides examples of the range of current applications and areas that could be developed in the future.

technologies in the public and health sectors. These social benefits are examined in this section. The final part examines environmental impacts and benefits of blockchain.

6.5.6.1. Social benefits

The promise of blockchain technology is to enable the efficient sharing of information with stakeholders while ensuring data integrity and protecting patient privacy.[682] Proponents hope that it will bring power to society and enable people to make positive decisions that improve their wellbeing and health and that of others around the world.

Maupin identifies a number of social use cases for blockchain utilisation.[683] These include:

- Financial services for currently unbanked and underbanked populations (remittances, micro-finance/micro-savings, community investment initiatives, etc);
- Off-grid financing of clean energy (e.g. solar in rural Africa and India);
- Digital identity and privacy management services - blockchain-powered cryptographic solutions to problems such as consumer privacy and mass data surveillance that also address countervailing risks of criminal abuse of blockchains' anonymity features for illicit purposes.[684]

Ballot rigging still persists in many parts of the world today.[685] Kim and Kang assert that blockchain technology can help to ensure that every eligible vote is counted accurately without any manipulation and this can greatly assist democracy.

A blockchain has interesting applications for intellectual property. Putting intellectual property on a blockchain allows the tracking of who uses it and can then be combined with a smart contract to ensure that when someone does use it, they also pay for it. An interesting example of this is work undertaken by the WEF in the Amazon Rainforest.[686] WEF is attempting to map the genome for each biological organism in the rainforest and then put this information onto a blockchain that has an in-built smart contract. This is being done so that anyone who uses this information will have to pay for it. The impacts of this blockchain are two-fold. Firstly, there will be money flows back to the countries where the information came from and, secondly, harmful uses of the rainforest will be reduced. In 2017, the UN's World Food Programme (WFP) conducted a successful pilot project in Jordan, where it used an Ethereum-based blockchain to manage cash-based transfers to 10,000 Syrian refugees living in the Azraq camp in Jordan.[687] Per WFP staff, the project has increased transparency and dramatically reduced costs. Whereas the WFP pays Jordanian banks a fee of 1.5 per cent to facilitate cash transfers, the fee to

[682] Mark Engelhardt, 'An introduction to blockchain technology in the healthcare sector (2017)', Technology Innovation Management Review, vol. 7, n°10. p22-34.
[683] Julie Maupin, 'The G20 countries should engage with blockchain technologies to build an inclusive, transparent, and accountable digital economy for all' (2017), Economics Discussion Papers, No. 2017-48, Kiel Institute for the World Economy (IfW), Kiel, available at http://hdl.handle.net/10419/163569 (last accessed on 20 December 2019).
[684] Djuri Baars, 'Towards self-sovereign identity using blockchain technology', Master Thesis, University of Twente, available at http://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf (last accessed on 20 December 2019).
[685] Kim K and Kang T., 'Does technology against corruption always lead to benefit? The potential risks and challenges of blockchain technology', OECD Global anti-corruption and integrity forum, available at https://www.oecd.org/cleangovbiz/Integrity-Forum-2017-Kim-Kang-blockchain-technology.pdf (last accessed on 20 December 2019).
[686] Dean Franklet et al., 'Public implementation of blockchain technology. Department of economics and finance' (2018), University of Canterbury. Available at https://ir.canterbury.ac.nz/bitstream/handle/10092/16353/Department%20of%20Economics%20working%20paper%201823.pdf?sequence=2&isAllowed=y (last accessed on 20 December 2019).
[687] Op.cit, Michael Pisa and Matt Juden, 'Blockchain and economic development: Hype vs. reality' (July 2017).

conduct transfers via the blockchain is nearly zero. The WFP estimates that, once the pilot is fully scaled up, it will pay only US$150 in monthly financial service fees, compared to US$150,000 today.

6.5.6.2. Public services

The EU Blockchain Observatory notes that blockchain capabilities can provide considerable benefits for the public sector.[688] Blockchain capabilities are beneficial for creating trust in information and processes in situations where there are large, heterogeneous sets of stakeholders or users.[689] Blockchain is also good at creating trusted audit trails of information and, depending on how a system is designed, it is also relatively easy to keep data both private and shareable. Because blockchains are jointly maintained, distributed systems with strong automation potential, they can be used to design efficient, inexpensive platforms, potentially leading to significant cost savings in public sector data processing while increasing the robustness of the platforms[690].

The Observatory describes four key areas where blockchain capabilities can be used in government. These include:

- *Securing and sharing data and records* - One of the most important groups of use cases for blockchain in government is around the verification of records and the sharing of data of various kinds. Relevant records include digital identities, title and asset registrations, educational certifications and eVoting;
- *Monitoring and regulating markets* - One of the key tasks of government is to regulate and monitor markets to protect consumers. Blockchain shared ledger capabilities can simplify data collection. Instead of self-reporting after the fact, regulators can more easily request real-time reporting from institutions like banks or manufacturers, potentially by 'plugging directly into' their systems or by developing a shared, blockchain-based platform. By using shared ledgers to reduce friction in data supply/gathering, governments greatly increase the amount of data they receive from regulated entities, as well as receive data from more sources;
- *Improving transactions, processes and transparency* – Blockchain can improve the ways in which governments transact and interact with citizens and companies. For example, governments collect tax payments generally based on self-reporting by individuals and companies. If governments have access to market data at the transaction level, they have the information they need to calculate the tax liabilities of the parties to the transaction. This should help fight fraud and recover lost revenue;
- *Efficiency improvements* - Blockchain can help increase efficiency and reduce costs in government operations. Whenever information is digitised, there are usually efficiency gains compared to paper-based processes. What makes blockchain relevant to government is the ability to digitise complex processes with a distributed architecture. Distributed systems can be significantly more efficient than the traditional, centralised model for the

[688] Op.cit, EU Blockchain Observatory and Forum, 'Blockchain for government and public services' (2018).
[689] Consensys, 'Blockchain for government and the public sector' (2019), https://consensys.net/enterprise-ethereum/use-cases/government-and-the-public-sector/ (last accessed on 20 December 2019).
[690] Open Access Government, '11 reasons for blockchain in public services' (2019), https://www.openaccessgovernment.org/blockchain-in-public-services/65941/ (last accessed on 20 December 2019).

simple reason that all users of the platform share the same infrastructure as opposed to each setting up their own siloed system.[691]

6.5.6.3. Healthcare

Blockchain capabilities offer considerable opportunities for social benefits from developments in the healthcare sector.[692] Potential benefits include utilisation in public healthcare management to enhance the exchange of healthcare records, for user-oriented medical research[693] and to address drug counterfeiting in the pharmaceutical sector.

Healthcare has traditionally been focused around data exchange between health professionals and business entities such as hospitals, doctors and other organisations.[694] There has been a recent push towards patient-driven interoperability, in which health data exchange is patient-mediated and patient-driven. Patient-centered interoperability, however, brings with it new challenges and requirements around security and privacy, technology, incentives, and governance that must be addressed for this type of data sharing to succeed at scale. Blockchain offers solutions to many of these barriers and the transition from institution-centric to patient-centric data sharing.

Sharing of healthcare data is a valuable source of intelligence to make healthcare systems smarter and improve the quality of healthcare service. The privacy of healthcare data is essential. Healthcare data is generally owned and controlled by the patient. Information is frequently scattered in different healthcare systems, which prevents data sharing and can place patient privacy at risks. Blockchain capabilities can ensure that patients own and control their healthcare data and also enable untrusted third-party to conduct research using patient data without violating privacy.[695]

The World Health Organisation identified that counterfeit drugs are a growing threat, particularly with increased internet sales of pharmaceuticals.[696] The WHO has received approximately 1,500 reports of fake and low-quality products, with antimalarials and antibiotics being the most-reported categories of risk. Section 6.2 provided an example of the use of blockchain capabilities to improve the security of pharmaceutical supply chains.[697]

By using blockchain, drug supply chain and pharmaceutical companies can use the distributed ledger to track and verify each drug's movement on the unchangeable record.[698] Blockchain records each time a drug swapped hands, assisting companies in

[691] However, decentralised systems can also be difficult to scale and less efficient. Stan Higgins, 'The EU is building a 'financial transparency gateway' (2017), https://www.coindesk.com/eu-developing-prototype-blockchain-platform-public-company-data (last accessed on 20 December 2019).
[692] Matthias Mettler, 'Blockchain technology in healthcare: The revolution starts here', available at https://ieeexplore.ieee.org/abstract/document/7749510 (last accessed on 20 December 2019).
[693] Xiao Yue et al., 'Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control' (2016), available at https://link.springer.com/article/10.1007/s10916-016-0574-6 (last accessed on 20 December 2019).
[694] William Gordon and Christian Catalini, 'Blockchain technology for healthcare: Facilitating the transition to patient driven interoperability' (2018), available at https://www.sciencedirect.com/science/article/pii/S200103701830028X (last accessed on 20 December 2019).
[695] Op.cit, Xiao Yue et al., 'Healthcare data gateways' (2016).
[696] WHO, Growing threat from counterfeit medicines (2018), https://www.who.int/bulletin/volumes/88/4/10-020410/en/ (last accessed on 20 December 2019).
[697] Gunjan Bhardwaj, 'Can blockchain solve pharma's counterfeit drug problem?' (April 2018), https://pharmaphorum.com/views-and-analysis/can-blockchain-solve-pharmas-counterfeit-drug-problem/ (last accessed on 20 December 2019).
[698] Mackenzie Garrity, 'Pharma companies consider blockchain to track counterfeit drugs' (2019), Hospital Review https://www.beckershospitalreview.com/pharmacy/pharma-companies-consider-blockchain-to-track-counterfeit-drugs.html (last accessed on 20 December 2019).

detecting tainted products before they reach consumers. But to get blockchain fully integrated, all companies must be on board, and some companies are hesitant to switch to a new infrastructure if they have a different system in place.

6.5.6.4. Environmental benefits

Section 2.2.4 provided a brief introduction to environmental issues concerning blockchain. This section provides a closer examination of the positive and negative environmental impacts of blockchain. Energy consumption associated with mining cryptocurrencies and other blockchain applications is increasing. Comparisons are often made with energy consumption in whole countries – Argentina[699], Denmark[700] and Switzerland[701] are often quoted examples. The technology is evolving, and energy efficiency will continue to improve. But early insights into limited areas of blockchain activity provide insights into the current magnitude of energy consumption.

The Digiconomist[702] and Cambridge University[703] created energy consumption indexes for Bitcoin and Ethereum. Both indexes generate similar values. Bitcoin blockchain size was estimated to be 184 gigabytes in size in Q3 2018.[704] In September 2018, energy consumption was estimated to be between 60 and 73 TWh. Energy consumption is not related to the number of transactions or blockchain size so it would be unwise to use the figures to extrapolate to other situations. Statista estimates suggest 18.5 per cent CAGR for growth in the size of the Bitcoin blockchain. If this 18.5 per cent growth figure for growth in the size of the Bitcoin blockchain is assumed and other relationships remain the same the Bitcoin blockchain will be 790 gigabytes in size in 2030.

Ethereum's energy consumption reached a maximum of 21 TWh in July 2018, since then it is estimated to have decreased to 7.4 TWh in September 2019, Digiconomist suggest this would create a carbon footprint of 3.5 million tonnes of CO2.

DataLight estimate that globally there are approximately 10,600 Bitcoin nodes maintaining transaction records.[705] Eight EU Member States were named in the top 20 countries (with more than 85 nodes), these included Germany (second with 2,016 nodes, USA had 2,625), France (third, 698), Netherlands (fourth, 527), United Kingdom (357), Finland (118), Ireland (106), Sweden (98), Lithuania (86). In total these 4,006 nodes represent a minimum of 38 per cent of global nodes.
However, estimating CO2 generation associated with this level of energy generation can be spurious. The volume of carbon created for generating electricity varies between

[699] 'Bitcoin energy demand in 2018 could match Argentina – Morgan Stanley' https://www.ft.com/content/93b22cb1-0346-38be-bebf-d2e676e19621 (last accessed on 24 January 2020) (subscription required).
[700] 'Mining Bitcoin uses More Energy than Denmark Study' (Nov 2018), https://www.thelocal.dk/20181106/mining-Bitcoin-uses-more-energy-than-denmark-study (last accessed on 20 December 2019).
[701] James Vincent, 'Bitcoin consumes more energy than Switzerland, according to new estimate' (2019), https://www.theverge.com/2019/7/4/20682109/Bitcoin-energy-consumption-annual-calculation-cambridge-index-cbeci-country-comparison (last accessed on 20 December 2019).
[702] Bitcoin Energy Consumption Index (2019), https://digiconomist.net/Bitcoin-energy-consumption (last accessed on 20 December 2019).
[703] Op.cit, James Vincent, 'Bitcoin consumes more energy than Switzerland, according to new estimate' (2019).
[704] Shanhong Liu, 'Size of the Bitcoin blockchain from 2010 to 2019' (2019), https://www.statista.com/statistics/647523/worldwide-Bitcoin-blockchain-size/ (last accessed on 20 December 2019.
[705] Matthew Bedham, 'Three countries host over 50 per cent of world's Bitcoin nodes' (2019), https://thenextweb.com/hardfork/2019/02/27/3-countries-50-perecent-Bitcoin-network/ (last accessed on 20 December 2019).

technologies and countries.[706] Iceland's geothermal power generation does not create CO2 emissions, Sweden only emits 13 grams of CO2 per kWh. The figure for the US is 489g per kWh.

Ethereum will be undergoing major development to enhance operations and reduce energy consumption, during its planned transitions to Proof-of-Stake, over the next 24 months.[707] The Ethereum community also intends to put sharding into practice. This will essentially break the network into a network of networks which each carry their own state and sync with the others. Due to the fact that Ethereum secures a massive amount of value already, these updates will be gradual and come as a series of tests running parallel to the network followed by an update of the software on the nodes.[708]
Some of the founders of Ethereum have even moved beyond doing work on that network and are deploying more flexible networks with consensus mechanisms that can be upgraded 'on the fly', and which include built in on-chain governance for upgrading essential parts such as hashing functions after deployment.

Very few of the newer blockchains are using older proof of work (PoW) methods. As a result, energy hungry PoW requirements will become less relevant over time.

Critical from a regulatory perspective is the fact that PoS networks secure the network via economic incentives. That means that PoS networks must have enough regulatory flexibility to develop into stable secure systems. If this flexibility and regulatory certainty does not exist in Europe, it is possible development could move to other parts of the world.

Major technology changes will be introduced in the next 12 to 18 months. This will develop the way major blockchains are able to scale and what consensus mechanisms are used.

Blockchain energy consumption is clearly environmentally detrimental. But blockchain is also forecast to have positive environmental impacts. The World Economic Forum has highlighted opportunities to harness blockchain to address 6 of today's most pressing environmental challenges.[709] These include climate change, natural disasters, biodiversity loss, ocean-health deterioration, air pollution and water scarcity.

WEF researchers declare blockchain provides a strong potential to unlock and monetise value that is currently embedded (but unrealised) in environmental systems. They identified more than 65 existing and emerging blockchain use cases for the environment through desk-based research and interviews with a range of stakeholders. Blockchain use case solutions that are particularly relevant across environmental applications tend to cluster around five cross-cutting themes:

- Enabling decentralised systems;
- Peer-to-peer trading of natural resources or permits;
- Supply-chain monitoring and origin tracking;
- New financing models, including democratizing investment;
- Realisation of non-financial value, including natural capital.

[706] Garrick Hilleman and Michel Rauchs, 'Global cryptocurrency benchmarking Study' (2017), available at https://www.researchgate.net/publication/317059599_2017_Global_Cryptocurrency_Benchmarking_Study (last accessed on 20 December 2019).
[707] Consensys, 'The Roadmap to Serenity' (2016), https://media.consensys.net/the-roadmap-to-serenity-bc25d5807268 (last accessed on 20 December 2019).
[708] James Ray, 'Sharding Roadmap', https://github.com/ethereum/wiki/wiki/Sharding-roadmap#strongphase-1strong-basic-sharding-without-evm (last accessed on 20 December 2019).
[709] World Economic Forum, 'Building blockchains for a better planet' (2018), available at http://www3.weforum.org/docs/WEF_Building-Blockchains.pdf (last accessed on 20 December 2019).

The challenge for innovators, investors and governments is to identify and scale these pioneering innovations both for people and the planet – while also making sustainability considerations central to wider blockchain development and use.

A key area where opportunities are forecast is carbon trading, where there has been scepticism over a lack of transaction visibility and traceability, differing standards and regulations across jurisdictions, and the potential for double counting.[710] Managing carbon markets on the blockchain has the potential to create efficiency in platforms and remove many of the carbon transaction constraints.[711]

An early pilot example is China's 'Carbon Credit Management Platform', developed by Energy-Blockchain Labs and IBM. The intent is that, with the introduction of smart contracts, the transparency, auditability and credibility of the Chinese carbon market can be increased. If successful, the approach could be broadened to other carbon markets around the world.

In jurisdictions that prefer a 'cap and trade' carbon-trading system, a blockchain application could potentially be used to automatically align licence creation, thus avoiding an over or undersupply of certificates, and thereby keeping market prices in a policy-agreed predefined range without the need for emergency or reactive interventions.

Currently, the trade in verifiable carbon-credit transactions is constrained by economies of scale. While verified carbon offsets are typically traded and verified in bulk amounts on the voluntary carbon market, the introduction of blockchain solutions enables carbon offsets to be attached at a microscale to individual products. Ben & Jerry's is piloting a blockchain platform to assign a carbon-credit price to each tub of ice cream sold, allowing consumers to offset their carbon footprint.[712]

6.6. Administrative and compliance burdens and costs

6.6.1. Methods to examine burdens and costs

The previous chapter developed policy options. Obviously, there will be costs associated with undertaking policy actions. These costs need to be considered in the light of benefits to consider whether a policy is economically sensible. However, policy intervention can also be considered on grounds such as social, democratic and environmental factors.

The European Commission Better Regulation Toolbox[713] provides thorough guidelines on cost benefit methods. Even in relatively small investigations, such as this component of the wider development of blockchain policies, the guidelines provide a robust underpinning for analysis. Tools #59 and #60 provide parameters and guidance for estimating administrative costs.

[710] Lisa Walker, 'This new carbon currency could make us more climate friendly' (2017), World Economic Forum Agenda blog, https://www.weforum.org/agenda/2017/09/carbon-currency-blockchain-poseidon-ecosphere (last accessed on 20 December 2019).
[711] Silke Elrifai et al., 'A Model Multilateral Treaty for the Encouragement of Investment in Climate Change Mitigation and Adaptation' (2019), Journal of International Arbitration, vol 36, n°1. Available at http://www.kluwerlawonline.com/abstract.php? area=Journals&id=JOIA2019004 (last accessed on 20 December 2019), p.71–94.
[712] Madeleine Cuff, Ben and Jerry's scoop blockchain pilot to serve up carbon-offset ice-cream (2018), https://businessgreen.com/bg/news/3033147/ben-and-jerrys-scoop-blockchain-pilot-to-serve-up-carbon-offset-ice-cream (last accessed on 20 December 2019).
[713] European Commission, 'Better Regulation Toolbox' (July 2017), http://www.emcdda.europa.eu/document-library/better-regulation-toolbox-european-commission_en (last accessed on 20 December 2019).

More thorough insights to costs of policy implementation were found by examining previous relevant DG CONNECT Impact Assessments since 2017 that had been positively received by the Regulatory Scrutiny Board.[714] Our review included examination of regulations to:

- Establish the European Cybersecurity Industrial, Technology and Research Competence Centre;[715]
- Establish the Digital Europe programme for the period 2021-2027;[716]
- Promote fairness and transparency for business users of online intermediation services;[717]
- Establish the European High-Performance Computing Joint Undertaking;[718]
- Establish a framework for the free flow of non-personal data in the European Union;[719]
- Establish the EU Cybersecurity Agency.[720]

Obviously no two policies will be exactly the same; but some policies use similar mechanisms for implementation. Some impact assessments provided clear costs for policy measures, in others, costs data was more obscure.

Some relevant DG GROW Impact Assessments were also examined.[721] Indeed, the most useful examples for this Study were obtained from DG GROW Impact Assessments concerning data storage servers and the single digital gateway.

6.6.2. Burdens and costs found in previous studies

One of the most useful previous impact studies for estimating costs of secondary legislation concerned a regulation to lay down eco-design requirements for servers and data storage products pursuant to Directive 2009/125/EC of the European Parliament

[714] List of impact assessments and the accompanying opinions of the Regulatory Scrutiny Board, https://ec.europa.eu/transparency/regdoc/?fuseaction=ia&year=&serviceId=10307&s=Search (last accessed on 20 December 2019). Nine impact assessments were available for 2017 to 2019. Six were relevant of loosely complementary to this Study.

[715] Opinion of the European Economic and Social Committee on 'Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres', (COM(2018) 630 final — 2018/0328 (COD)) EESC 2018/04805, OJ C 159, 10.5.2019, p. 63–67, available at https://eur-lex.europa.eu/search.html?qid=1576233125975&PROC_NUM=0328&DB_INTER_CODE_TYPE=OLP&type=advanced&PROC_ANN=2018&lang=en (last accessed on 24 January 2020).

[716] Opinion of the European Committee of the Regions on the 'Digital Europe programme (2021-2027) JO C 86 du 7.3.2019, p. 272–281, available at https://eur-lex.europa.eu/search.html?qid=1576233174117&PROC_NUM=0227&DB_INTER_CODE_TYPE=OLP&type=advanced&PROC_ANN=2018&lang=en (last accessed on 24 January 2020).

[717] Regulation (EU) 2019/1150 OF THE European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediate in services, OJ L 186/57, 11/07/19, available at https://eur-lex.europa.eu/search.html?qid=1576233186463&PROC_NUM=0112&DB_INTER_CODE_TYPE=OLP&type=advanced&PROC_ANN=2018&lang=en (last accessed on 24 January 2020).

[718] Council regulation (EU) 2018/1488 of 28 September 2018 establishing the European High Performance Computing Joint Undertaking, OJ L 251/1, 08.10.2018, available at https://eur-lex.europa.eu/search.html?qid=1576233191287&PROC_NUM=0003&DB_INTER_CODE_TYPE=NLE&type=advanced&PROC_ANN=2018&lang=en (last accessed on 24 January 2020).

[719] 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, OJ L 303/59, 28/11/2018, available at https://eur-lex.europa.eu/search.html?qid=1576233195992&PROC_NUM=0228&DB_INTER_CODE_TYPE=OLP&type=advanced&PROC_ANN=2017&lang=en (last accessed on 24 January 2020).

[720] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), available at https://eur-lex.europa.eu/search.html?qid=1576233214010&PROC_NUM=0225&DB_INTER_CODE_TYPE=OLP&type=advanced&PROC_ANN=2017&lang=en (last accessed on 24 January 2020).

[721] The list of impact assessments records seven submissions from DG GROW in 2018 and 2019.

and of the Council.[722] This estimated administrative costs of implementing measures in the form of a directive at €4.7 million, of which €720.000 for administrative work on the amendment and development of the new directive and €4 million for transposition by Member States.

This study was also one of the few to provide insights to predicted policy impact. Server electricity consumption after ten years in 2030 under the do nothing (or baseline) situation was 47.9 TWh/year. A guidance-based option (with changes in power supply units) was expected to reduce electricity consumption by 1.8 TW/h/year to 46.1 TWh/year in 2030. These two elements, guidance and technical changes, thus achieved a policy impact of 3.7 per cent.

One study proposed the utilisation of information and guidance procedures similar to those prescribed in this study. This study, undertaken for DG GROW, proposed the development of a single digital gateway to improve online availability, quality and findability of information and assistance services on EU rights and national rules concerning the cross-border operations and movement in the EU.[723] The study found:

- The development of information and guidance, with translation would incur an initial cost of €1 million and recurrent annual costs of €500,000;
- The development of a network of European Consumer Centres would initially cost the EU €6 million in grants. With support of €5 million from national administrations.

A search of 13 complementary DG CNECT and DG GROW Impact Assessments, yielded few useful insights to costs and impacts. But the few that were relevant are useful and pertinent since they have been rigorously considered and then approved by the Regulatory Scrutiny Board. These two observations are useful, but documentation does not contain detailed information about implementation activities. The next section therefore also includes more granular analysis of the costs associated with the implementation of policy options.

6.6.3. Likely costs for the proposed policies

Utilising the preceding cost estimates approved by the Regulatory Scrutiny Board and utilising salary information it is possible to provide cost estimates for the proposed policy options (i.e. 'Wait and See', Regulatory Guidance and Secondary Legislation). The key policy implementation activities and timespans for implementation proposed in Chapter 5 are provided in Table 4.

[722] European Commission, 'Commission Staff Working Document, Executive Summary of the Impact Assessment Accompanying the document Commission Regulation laying down Ecodesign requirements for servers and data storage products pursuant to Directive 2009/125/EC of the European Parliament and of the Council and amending Commission Regulation (EU) N°617/2013' (15 March 2019), available at https://ec.europa.eu/transparency/regdoc/rep/10102/2019/EN/SWD-2019-105-F1-EN-MAIN-PART-1.PDF (last accessed on 20 December 2019).

[723] European Commission, 'Commission Staff Working Document, Impact Assessment Accompanying the document Proposal for a regulation of the European parliament and of the Council on establishing a single digital gateway to provide information, procedures, assistance and problem solving services and amending Regulation (EU) No 1024/2012' (2 May 2017), available at https://ec.europa.eu/transparency/regdoc/rep/10102/2017/EN/SWD-2017-213-F1-EN-MAIN-PART-3.PDF (last accessed on 20 December 2019).

Table 4 - Implementation activities

	Wait-and-See	Regulatory Guidance	Secondary Legislation	Implementation Activities
Legal issues regarding blockchain technology in general				
Responsibility for legal compliance and liability [a]	X			
Potential barriers in sectoral legislation	X			
The protection of fundamental legal principles and mandatory rules	X			
Tension between blockchain reality & legal reality	X	X		EC lead development of guidance on best practices for aligning off-chain and on-chain information. Consultation with national government and stakeholders. 1 to 2 yrs
Legal issues regarding smart contracts				
Application of Contract Law [b]	X			
The need for written form of the contract	X			
Smart contracts and Consumer Law [c]	X			
Smart contracts and pseudonymity (see 5.3.4)		X		EC lead development of guidance on standard contractual clauses. Consultation with national govt. and stakeholders. 1 to 2 yrs
Smart contracts and jurisdiction	X			
Capacity to contract and protection of minors	X			
Opacity	X			
Smart Contract Arbitration Mechanisms (see 5.3.8)		X		EC lead development of guidance for standard arbitration clauses. Consultation with national govt. and stakeholders. 1 to 2 yrs
Notarisation	X			
Legal issues regarding utility tokens				
Lack of legal certainty and regulatory fragmentation (see 5.4.1)		X	X	Development of secondary legisalation (3 to 4 years) and the EC lead development of guidance on how existing legal frameworks apply to utility tokens. Consultation with national government and stakeholders. 1 to 2 yrs
Consumer protection (inc. prospectus reqrmnts) (see 5.4.2)	X	X		EC lead development of guidance on how consumer protection law applies. Consultation with national govt. and stakeholders. 1 to 2 yrs
Trading on secondary markets (see 5.4.3)		X		EC lead development of guidance for standards to be adopted by industry. Consultation with national govt. and stakeholders. 1 to 2 yrs

[a] Relevant national enforcement organisations should already have been be involved in enforcing ICO non-compliance.

[b] Possible guidance that might need to be clarified by the Court of Justice of the European Union or a revision of the Rome Regulation is not included, see Section 5.3.1.

[c] "Wait and see" is recommended as the primary option in. It is suggested there could be benefits in including blockchain considerations of the next revision of Consumer Rights Directive. Since these would form part of more extensive revision activities they are not considered or costed separately.

[*] Please note that for the purposes of this matrix, the policy option of standard contractual clauses is considered under "Regulatory Guidance".

Several of the policy options concern a 'wait and see' approach. This option requires the Commission to monitor developments. We believe this monitoring would probably be undertaken during the course of the everyday activities of relevant European Commission units. No costs are therefore associated with 'wait and see' activities.[724]

The six options all include the development of guidance materials. The development of these guidance materials would in all cases be led by the European Commission. Salaries for relevant personnel have therefore been obtained for the European Commission.[725] Three Commission employment levels are envisaged for the development of guidance materials:

[724] Please note that certain suggested approaches (e.g. regulatory sandboxes and the funding of research) were categorised under "Other" (see Table 3), and were not assessed in the context of the economic analysis carried out in this chapter.

[725] European Commission salaries, https://www.glassdoor.co.uk/Salary/European-Commission-Brussels-Salaries-EI_IE147109.0,19_IL.20,28_IM992.htm (last accessed on 21 January 2020).

- Policy Officer: €72,827 per annum
- Administrator: €51,708 per annum
- Secretary: €33,660 per annum

The development of guidance materials also requires consultation with national government and other stakeholders. Eurostat provides information about the average annual earnings of 'managers' across all EU Member States.[726] These suggest the salary cost of one week time input by a manager during engagement activities would be €973.[727]

The development of guidance materials is estimated to be between one and two years. Calculations include sensitivity analysis components by examining costs for one and two-year implementation time periods.

We envisage that the development of guidance materials will be undertaken by three European Commission personnel – a Policy officer, an administrator and a secretary. Annual salary costs for these three positions are approximately €164,200.

During engagement activities we envisage that representatives from the Member States will be consulted together with representatives from 20 other organisations. One week of input is envisaged to review materials, consult within their organisation, prepare a response for the Commission and undertake interviews or attend workshops. 48 weeks input from managerial staff in these organisations would be approximately €46,700. We envisage that a one-year policy implementation period would require one round of consultation. Two rounds of consultation are envisaged if implementation takes two years.

In total one-year development of policy guidance options will costs of €210,900. The Commission will incur 78 per cent of these costs (€164,200) and other organisations €46,700. In comparison the impact analysis study for the single digital gateway suggested recurrent annual costs of €500,000 per annum,[728] but this was for a policy that had much greater interaction with 28 EU Member States stakeholders. The estimate suggested for guidance development therefore appears reasonable.

Two-year policy guidance development will incur total costs of €421,800.

In relation to *legal issues regarding blockchain technology in general* a 'wait and see' approach is proposed. As noted above we believe this monitoring would probably be undertaken during the course of the everyday European Commission activities. Section 5.2.1 noted that responsibility for legal compliance was already vested in the relevant authorities in each EU Member State. These national enforcement organisations should already have been be involved in enforcing ICO non-compliance.

In the *general area developing legislation for blockchain technology*, one guidance action is suggested to develop and share best practices for aligning off-chain and on-chain information. Using the previous guidance development estimates we envisage costs of €210,900 if implemented in a single year and €421,800 if implemented over two years.

[726] Eurostat. 2020, Mean annual earnings by sex, age and occupation - NACE Rev. 2, [earn_ses14_28] €43,777, available at http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=earn_ses14_28&lang=en (last accessed on 23 January 2020)
[727] European Commission and Eurostat data concerns salaries received by employees. It does not include employment taxes and other contributions. Nor do salary costs include employment costs such as accommodation and utilities in the workplace.
[728] After initial costs of €1 million.

In the area of policies for *smart contracts*, two regulatory guidance options are suggested. It is probable these two areas (concerning pseudonymity and arbitration) could be undertaken in a single guidance package. Therefore, we estimate costs of €210,900 if implemented in a single year and €421,800 if implemented over two years.

The final policy area examines *utility tokens*. This is the only area that envisages the introduction of secondary legislation. As noted earlier, the development of secondary legislation for the Directive on eco-design requirements for servers and data storage products is estimated to have cost €4.7 million to introduce. This is therefore used as a guideline price for secondary legislation concerning utility tokens.

Three guidance policies are suggested for utility tokens. Once again it is envisaged these could be developed concurrently by the European Commission team leading the development of guidance materials. The preceding approach has been adopted for these, suggesting a cost of €210,900 if implemented in a single year and €421,800 if implemented over two years.

Of course, it is possible that the six guidance elements proposed for smart contracts and utilities could be joined together into a single guidance structure. If this was the case, it is possible that significant implementation savings could arise. But we believe the three core components to the Study (general issues, smart contracts and utility tokens) are significantly different enough to warrant each area developing guidance materials separately.

Thus, total development costs for three groups of guidance activities are likely to be about €632,700 if implemented in a single year and €1.265 million if implemented over two years. Legislation for consumer protection for utility tokens will also add €4.7 million.

Table 5 - Cost estimates for the implementation[729] of policy options

	Implementation Activities	Implementation costs
Legal issues regarding blockchain technology in general		
Responsibility for legal compliance and liability [a]		
Potential barriers in sectoral legislation		
The protection of fundamental legal principles and mandatory rules		
Tension between blockchain reality & legal reality	EC lead development of guidance on best practices for aligning off-chain and on-chain information. Consultation with national government and stakeholders. 1 to 2 yrs	€210,900 one year €421,800 two years
Legal issues regarding smart contracts		
Application of Contract Law		
The need for written form of the contract		
Smart contracts and Consumer Law		
Smart contracts and pseudonymity (see 5.3.4)	EC lead development of guidance on standard contractual clauses. Consultation with national government and stakeholders. 1 to 2 yrs	€210,900 one year €421,800 two years
Smart contracts and jurisdiction		
Capacity to contract and protection of minors		
Opacity		
Smart Contract Arbitration Mechanisms (see 5.3.8)	EC lead development of guidance for standard arbitration clauses. Consultation with national government and stakeholders. 1 to 2 yrs	
Notarisation		
Legal issues regarding utility tokens		
Lack of legal certainty and regulatory fragmentation (see 5.4.1)	Development of secondary legisalation (3 to 4 years) and the EC lead development of guidance on how existing legal frameworks apply to utility tokens. Consultation with national government and stakeholders. 1 to 2 yrs	€4.7 million
Consumer protection (inc. prospectus reqrmnts) (see 5.4.2)	EC lead development of guidance on how consumer protection law applies. Consultation with national government and stakeholders. 1 to 2 yrs	€210,900 one year €421,800 two years
Trading on secondary markets (see 5.4.3)	EC lead development of guidance for standards to be adopted by industry. Consultation with national government and stakeholders. 1 to 2 yrs	

6.6.4. Likely timescale for the proposed policies

By examining legislative timescales[730] for items presented in the European Parliament, it is possible to validate the likely timeline for the development of regulatory guidance measures and secondary legislation presented in the previous section. Table 6 provides an overview of relevant timelines for legislation associated with the Connected Digital Single Market.

Table 6: Legislative Timescales in the Connected Digital Single Market

	First Instance	Actions Taken
5G Action Plan	**June 2016:** Adopted agenda advocating deployment of high-capacity fixed and wireless broadband connectivity across Europe.	**September 2016:** Proposals put forward for three legislative and one non-legislative measures. **February 2018:** 5G observatory established. **March 2018:** Agreement on spectrum.

[729] Implementation at EU level.

[730] 'The legislative train schedule for the Connected Digital Single Market', http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-5g-action-plan (last accessed on 20 December 2019).

European Cybersecurity Competence Centers September 2018	**Sept 2017:** European Commission adopted a cybersecurity package.	**November 2017:** Council welcomed the intention to set up a cybersecurity competence network. **December 2018:** Draft report published. **March 2019:** Report approved by Parliament.
Artificial Intelligence for Europe May 2018	**January 2017:** European Parliament asked European Commission to assess the impact of Artificial Intelligence.	**April 2018:** 25 European countries signed a declaration of cooperation on Artificial Intelligence. **May 2018:** Adopted a Communication on Artificial Intelligence for Europe. **April 2019:** Published ethics guidelines for trustworthy Artificial Intelligence.
Digitalising European Industry	**January 2016:** European Parliament asked European Commission to propose rules fit for the digital age.	**April 2016:** European Commission published communication on digitalising European Industry. **June 2017:** Adopted a resolution on developing an integrated industrial digitalisation strategy. **March 2018:** A number of priorities were highlighted to reap the full benefits of digital transformation.
Online Platforms: Disinformation June 2017	**March 2015:** European Council stresses need to counter 'Russia's ongoing disinformation campaigns.'	**June 2017:** Called to analyse the legal framework with regard to fake news. **October 2017:** Set up a high-level expert group. **September 2018:** Code of Practice published. **Mach 2019:** Rapid Alert System, to share data of campaigns, launched. **June 2019:** Communication on implementation of action plan. **October 2019:** Adopted a resolution on foreign electoral interference and disinformation. Published first annual self-assessment reports by signatories of the Code of Practice.

The table highlights that:

- A 5G Observatory was established 21 months after first Parliamentary discussion;
- A European cybersecurity report was approved 18 months after first Parliamentary discussion;
- AI Ethical Guidelines were published 27 months after first Parliamentary discussion;
- A code of practice for online platforms and disinformation was published 42 months after first Parliamentary discussion.

Although no clear pattern is discernible, we believe it would not be unreasonable to adopt a one to two year period for the implementation of the policy recommendations proposed in this Study.

6.7. The impact of policy options proposed at the workshop

6.7.1. Introduction

The previous section highlighted that Better Regulation guidelines require the costs of policy implementation and impacts to be monetised where possible. The previous sections also examined costs. This section provides insights into policy impacts by applying probable policy impacts to the baseline forecasts developed from the views of Delphi participants presented earlier in the Study. The final section considers the relative difference between costs and benefits.

6.7.2. Policy impacts

Having established costs for implementation (€632,700 if implemented in a single year and €1.265 million if implemented over two years plus legislative costs estimated at €4.7 million), this section tentatively provides estimates of possible impacts for policies.

In our examination of 13 relevant Commission impact assessments[731] related to legislation and technologies complementary to blockchain, we were only able to find one report that provided forecasts about the policy impacts. This concerned regulations to establish eco-design requirements for servers and data storage. Server electricity consumption in 2030, ten years after the introduction of policies, under the do nothing (or baseline) situation was 47.9 TWh/year. An information guidance-based option (with changes in power supply units) was expected to reduce electricity consumption by 1.8 TW/h/year to 46.1 TWh/year in 2030. These two elements – guidance and technical changes – thus achieved a policy impact of 3.7 per cent.

The use of guidance and information dissemination policies in the eco-design regulation is a similar approach to the regulatory guidance proposed in this Study. It is therefore assumed that guidance policy options proposed for this Study will have a similar impact and be less than 3.7 per cent.[732] Impact figures of two and three per cent are adopted and applied to the baseline model.

Section 6.6.6.4 noted that on the basis of previous regulations developed by the European Parliament, it was probable that the proposed policy options would not be introduced for two years. It is therefore assumed that policy impact in the baseline model will not take place until 2022.

The impact of policies does not remain constant.[733] Over time, the impact of policies can decline and/or policies can be superseded by new regulations and legislation. A policy decay function has therefore been introduced into baseline impact calculations. This is an innovative approach developed by Callander and Martin.[734] In the impact assessment it is assumed that the impact of policy declines by 20 per cent per annum. Thus, policy has 100 per cent impact in the first year,[735] 80 per cent in year two, etc.

---

[731] DG CONNECT: nine assessments 2017 to 2019, six relevant. DG GROW: seven impact assessments 2018 and 2019.

[732] The ecodesign policies introduced technical changes alongside the development of guidance. The separate impacts of the two elements was not distinguished. We therefore assume a maximum possible guidance policy impact of three per cent, since the technical change elements most have had some impact to be included in the regulations.

[733] UK CDC, 'Evaluating Policy Impact' (2017), available at https://www.cdc.gov/injury/pdfs/policy/Brief%205-a.pdf (last accessed on 20 December 2019).

[734] Steven Callander and Gregory Martin, 'Dynamic Policymaking with Decay. American Journal of Political Science' (2016), vol 61, issue 1. Available at https://onlinelibrary.wiley.com/doi/abs/10.1111/ajps.12258 (last accessed on 20 December 2019).

[735] It could be argued that policy implementation takes some months to achieve a full impact due to background and preparatory work having to be completed before policy launch and/or dissemination.

6.7.3. The impact of policies on the general blockchain baseline model

Three of the four policy options proposed for 'legal issues regarding blockchain technology in general' are 'do nothing' or wait and see options. Regulatory guidance is suggested to address tension between blockchain reality and legal reality. Guidance suggested included the Commission or industry groups developing guidance on best practices.

The preceding section noted that the impact of guidance options would be estimated at the level of two and three per cent. Policies would not be introduced until 2022 and policy decay would occur at 20 per cent per annum.

Section 6.5.3.1 provided insights to Delphi participants views about trends in the growth of blockchain market expenditure. The majority of participants thought that the Critical Future forecast was too low. A ten cent per cent increase in this forecast was therefore made in Figure 15. This 'S-shaped' adoption curve predicted investment of €10.06 billion a year in 2030.

Figure 21 provides presents forecast for the impact of regulatory guidance policy at two per cent between 2020 and 2030.[736] The solid black line is the Delphi participants forecast taken from Figure 15. The finely dotted line shows the impact of regulatory guidance policy at two per cent with a decline in the impact of the policy after it is first introduced in 2022. The upper dotted line presents the same impact but without a policy decay function.

Figure 21 - Two per cent impact of regulatory guidance on blockchain expenditure

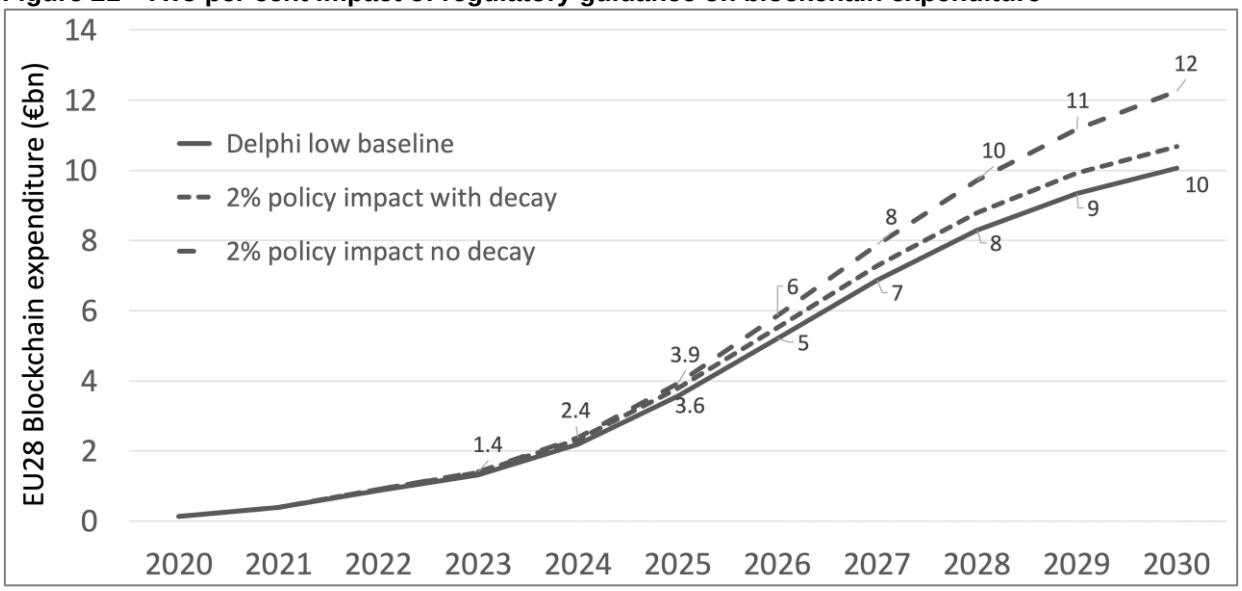


Figure 21 provides insights to policy impact of two per cent. Table 7 presents results of sensitivity analysis if the impact of policy was three per cent. Once again 'with' and 'without' policy decay components are presented. The final column of the table presents the cumulative difference (across eight years 2022 to 2030) in calculations. This shows that a conservative policy impact of two per cent per annum with a decay in the impact of the policy would increase total blockchain expenditure between 2022 and 2030 by €2.89 billion. If the impact of guidance was three per cent impact (with decay) increases to €4.38 billion. Higher returns can be observed if the impact of policy does not decay.

[736] The rationale for two and three per cent impact parameters, derived from the impact assessment developing regulations to establish eco-design requirements for servers and data storage, were described in the previous section.

Table 7 - Two and three per cent impact of regulatory guidance on blockchain expenditure (€ bn) in 2025 and 2030

	2025 (€bn /annum)	2030 (€bn /annum)	2022 to 2030 cumulative difference (€bn)
Delphi baseline forecast (€ bn per annum)	€3.56 bn	€10.06 bn	-
Cyprus			
Two per cent policy impact with decay	€3.78 bn	€10.68 bn	€2.89 bn
Two per cent policy impact without decay	€3.93 bn	€12.26 bn	€7.81 bn
Cyprus			
Three per cent policy impact with decay	€3.90 bn	€11.00 bn	€4.38 bn
Three per cent policy impact without decay	€4.13 bn	€13.52 bn	€12.14 bn

Section 6.5.3.1 noted a high degree of convergence in Delphi study participants views about the rate of return on blockchain expenditure. This estimated a return of 10 per cent rate of return.

This would suggest that even at the lowest level of cumulative increase (€2.89 billion) cumulative returns on investment between 2022 and 2030 would be €289 million. Section 6.5.4 highlighted that in the first instance these relatively significant returns will arise for investors. Benefits to Exchequers and society will arise from taxes on these returns if they are declared as profits.[737] Benefits for citizens and society will also arise if those investing in blockchain pass on the benefits of higher returns through reducing the cost of goods and services for consumers. Section 6.5.6 provided an overview of further social benefits that might arise if the regulatory guidance policy enhanced the use of blockchain for social good in areas such as public services and healthcare.

Section 6.5.6.4 highlighted that increased investment and thus use of blockchain will not necessarily have a detrimental environmental impact. Increased energy consumption that might arise from greater blockchain use will only have a detrimental impact if power generation creates CO2 emissions. Power generation in Iceland does not create CO2 emissions[738] and other countries have targeted a reduction in emissions to zero.

6.7.4. The impact of policies on the smart contract baseline model

Section 6.5.3.1 noted that domestic Member State contract law applies to smart contracts where these qualify as legal contracts. It was thus asserted that no specific issues require a supranational action. One specific area examined in some depth was the validity and enforcement of (smart) contracts for cross-border transactions.

Section 6.5.4 noted that intra-EU trade in goods (rather than trade within a single Member State) was selected for baseline analysis because this is the tier at which EU intervention could have the greatest benefit. Subsidiarity and proportionality principles authorise intervention by the EU when the objectives of an action cannot be sufficiently achieved by the Member States. It was therefore considered erroneous to examine trade

[737] The increased level of expenditure might also lead to additional Exchequer income in VAT payments for blockchain expenditure.
[738] Op.cit, Garry Hileman and Michel Rauch, 'Global cryptocurrency benchmarking study' (2017).

within in a single Member State because legislation and regulations could be established by the government of that country.

Seven of the nine policy options proposed for 'legal issues regarding smart contracts' are 'do nothing' or wait and see options. Regulatory guidance is suggested in two areas – pseudonymity and arbitration mechanisms. Suggested pseudonymity policy options include elaborating standard contractual clauses related to identification and encouragement for the development of digital and/or self-sovereign identity systems. Recommended arbitration mechanisms in the collaboration with relevant stakeholders and businesses at national and supranational levels to support blockchain use. These types of guidance options are similar to those used to estimate costs and impacts above.

Like the preceding baseline analysis, the impact of guidance policies is investigated at levels of two and three per cent. The guidance options will forecast to be introduced in 2022. The impact of guidance with and without decay (at 20 per cent per annum) will be investigated.

Section 6.5.4. provided insights to Delphi participants views about trends for the impact of blockchain in intra-EU trade. In this section, the green line in Figure 15 provided the 'S-shaped' adoption curve selected by Delphi participants who forecast blockchain market saturation by 2034. The curve provided baseline forecasts of savings achieved by smart contract use with a saving of €4.60 per transaction which the Delphi participants was about right.

Figure 22 - Two per cent impact of regulatory guidance on blockchain enabled intra-EU trade in goods

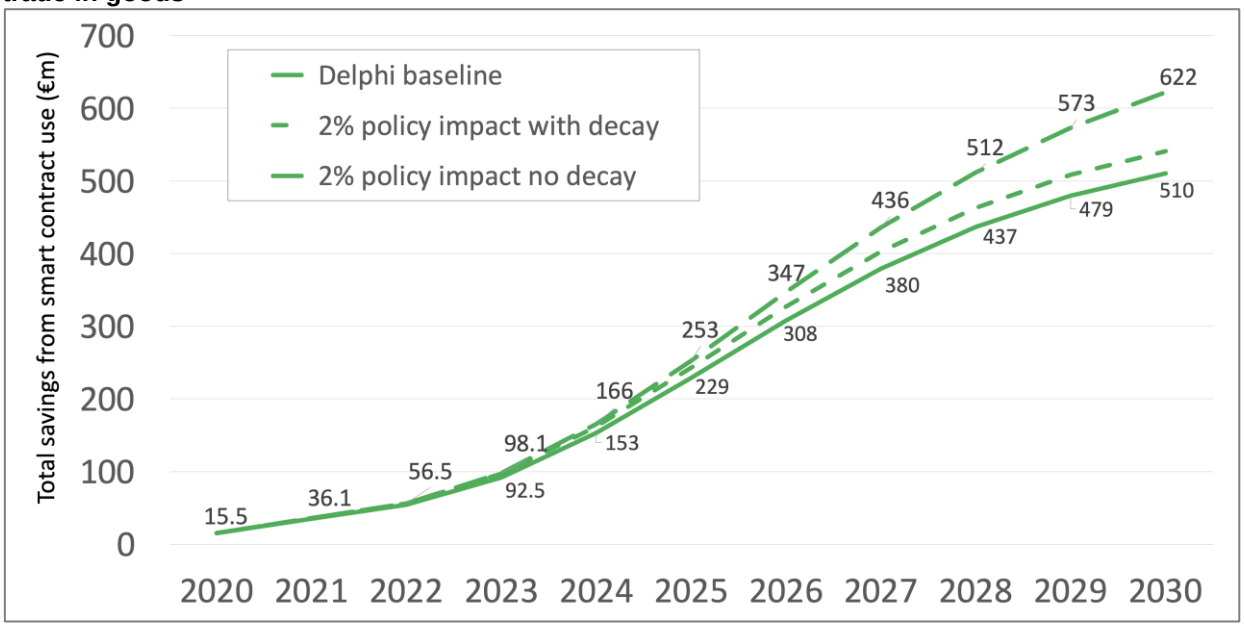


Figure 22 provides insights to policy impact of two per cent. Table 8 presents results of sensitivity analysis if the impact of policy was three per cent. Once again 'with' and 'without' policy decay components are presented. The final column of the table presents the cumulative difference (across eight years 2022 to 2030) in calculations. This shows that a conservative policy impact of two per cent per annum with a decay in the impact of smart contracts on intra-EU trade would lead to transaction savings between 2022 and 2030 of €160 million. If the impact of guidance was three per cent impact (with decay) increases to €242 million. Higher returns can be observed if the impact of policy does not decay.

Table 8 - Two and three per cent impact of regulatory guidance on blockchain enabled intra-EU trade in good (€ million) in 2025 and 2030

	2025 (€m per annum)	2030 (€m per annum)	2022 to 2030 cumulative difference (€m)
Delphi baseline forecast (€m per annum)	€229 m	€510 m	-
Two per cent policy impact with decay	€243 m	€542 m	€160 m
Two per cent policy impact without decay	€253 m	€622 m	€421 m
Three per cent policy impact with decay	€250 m	€558 m	€242 m
Three per cent policy impact without decay	€263 m	€686 m	€654 m

Figure 22 and Table 8 highlight the savings that could be achieved if guidance impact forecasts are correct. As noted previously, in the first instance these returns will arise for those utilising blockchain. Benefits to Exchequers and society will arise from taxes on these returns if they are declared as profits. Benefits for citizens and society will also arise if those utilising blockchain to achieve intra-EU trade savings pass on some of the savings in the form reduced costs for goods to consumers.

Section 6.5.6.4 highlighted that increased use of blockchain will not necessarily have a detrimental environmental impact. Increased energy consumption that might arise from greater blockchain use will only have a detrimental impact if power generation creates CO2 emissions. Many countries have targeted zero emissions for power generation.

6.7.5. The impact of policies on utility tokens

Section 6.5.5 noted difficulties in defining a 'utility token' and in providing functional and legal criteria for utility tokens. In addition, it was noted that tokens can take on a hybrid nature overlapping with financial tokens. With fluidity in definitions and parameters it is not surprising that our team could not find any forecasts for future growth and forecasts for utility tokens. It has not therefore been possible to replicate the preceding baseline analysis to examine the impact of policies.

Section 6.5.6 provided a flavour of some of the social benefits that might arise from utility tokens. The magnitude of these benefits was not as great as the preceding two examples. But previous sections examining complementary blockchain areas has revealed that even a relatively small increase in use of utility tokens will be likely to cover the costs and burden of policy implementation, which for this option with secondary legislation and guidance is estimated to be 8.2 million over five years.

6.7.6. The difference between policy costs and benefits

Above, insights were provided to probable costs associated with undertaking policy actions. This section has examined policy impacts. It is therefore now possible to compare policy action costs with impacts.

Unlike other impact assessments reviewed in the course of this Study, a single set of policies has been proposed for the key areas examined in this Study.[739] A single cost for

[739] Other studies examined have a 'do nothing' option, this can be aligned by the baseline forecasts in this Study. Policy options are then proposed on increasing scales of intensity, this is usually matched by costs.

policy development and implementation (over one and two years) is therefore allocated to the three areas (see Table 9).

Table 9 - Costs and benefits associated with the three key blockchain areas examined

	Implementation cost over 2 years	Lowest cumulative difference 2022 to 2030	Highest cumulative difference 2022 to 2030
Policy proposals for blockchain technology in general	€210,900 one year €421,800 two years	€ 2,890 m	€12,140 m
Policy proposals for smart contracts	€210,900 one year €421,800 two years	€ 160 m	€ 654 m
Policy proposals for utility tokens	€4.922 m over two to five years	unknown	unknown

Economic analysis and input from Delphi participants have revealed the high levels of growth and benefits expected from blockchain. Growth until 2030 is so high that even if policy options have a small percentage impact on markets the economic and associated social impacts will be far greater than the cost of policy implementation. This should not be regarded as a 'carte blanche' to introduce any policy. Care will still be required to ensure that policies enhance catalysts for blockchain development (Section 6.2.2) and overcome barriers to blockchain adoption (Section 6.3).

6.8. Monitoring and evaluation

Previous impact assessments[740] provide useful examples of monitoring and evaluation methods that have been approved by the Regulatory Scrutiny Board which could be suitable for the proposed implementation of policies.

The establishment of the new legal instruments will obviously trigger monitoring activities. Legislation should include explicit clauses to monitor the key performance indicators (KPIs). Also, an explicit evaluation and review clause, by which the European Commission will conduct an interim evaluation should also be included in the legal instrument, in order to measure the impact of the instrument and its added value.

The European Commission will subsequently report to the European Parliament and the Council on its evaluation. The Commission's Better Regulation methodology for evaluation should be utilised. These evaluations will be conducted with the help of targeted, expert discussions, studies and wide stakeholder consultations.

If a blockchain regulatory guidance centre or similar entity is established, the Executive Director of the legal entity should present to the Governing Board an ex-post evaluation of Centre's guidance and/or networking activities every year. The legal entity should also prepare a follow-up action plan regarding the conclusions of retrospective evaluations and report on progress annually to the Commission.

The Governing Board will be responsible to monitor the adequate follow-up of such conclusions. Alleged instances of maladministration in the activities of the legal body

[740] List of impact assessments and the accompanying opinions of the Regulatory Scrutiny Board (2018), https://ec.europa.eu/transparency/regdoc/?fuseaction=ia&year=&serviceId=10307&s=Search (last accessed on 20 December 2019).

may be subject to inquiries by the European Ombudsman in accordance with the provisions of Article 228 of the Treaty.

6.9. Conclusion

This chapter has provided a socio-economic review and forecasts for blockchain up to 2030. Many commentators have asserted that blockchain will contribute to economic growth and foster local social development. This Study is thought to be one of the first to examine socio-economic forecasts in the public domain and share them with experts using Delphi methods to validate and/or adjust forecasts to more accurately reflect the views of blockchain professionals.

The first section of the chapter considered the underlying characteristics of blockchain opportunities and the drivers and barriers to achieving socio-economic impacts. It is these catalysts and impediments to development that should be addressed by policies to enhance growth and competition and reduce barriers and detrimental impacts of blockchain. During the research, 'legal certainty' and 'regulation clarity' were regarded as key catalysts for blockchain development. Interestingly, since this certainty and clarity does not currently exist in all areas, the same two issues were also included as key barriers by some observers.

The Study examined the stakeholder groups and sectors most likely to be impacted by blockchain. A number of studies assert that the largest impacts of blockchain will arise in the financial sector. The World Economic Forum highlighted that many liquid and illiquid financial assets remain highly dependent on intermediating institutions to discover and connect buyers and sellers, often based on networks of pre-existing relationships with other institutions. Blockchain capabilities have the potential to support market making and disintermediation. A number of financial platforms are emerging that realign how buyers and sellers are connected for various products and transactions, generally improving the efficiency of those markets.

Forecast impacts of blockchain in financial and other sectors are significant. For example, a Santander Innoventures report asserts that distributed ledger technology could reduce banks' infrastructure costs attributable to cross-border payments, securities trading and regulatory compliance by between €13.8 to €18.4 billion per annum by 2022. The World Food Programme conducted a successful pilot project in Jordan using an Ethereum-based blockchain to manage cash-based transfers to refugees. They estimate that, once the pilot is fully developed, fees for financial services will be reduced 1,000 fold – from US$150,000 to US$150 per month.

Having provided a socio-economic overview of blockchain forecasts and the nature and scale of the blockchain opportunity, the Study developed baseline forecasts. These baselines were developed to investigate the impact of policy options on blockchain market expenditure and intra-EU trade facilitated by smart contracts.

The baseline models are a meta-analysis best estimate of the future. Baseline models were developed during two rounds of Delphi research with experts. The first round consisted of email contact and interviews with more than 200 global experts with wide ranging interests in blockchain. The second round was undertaken during a Commission-hosted workshop in Brussels in December 2019. The baseline forecasts to 2030 envisage how key blockchain opportunities might evolve without policy action at EU level.

Using feedback from the two rounds of Delphi surveys it was possible, using 'S-shaped' adoption methodologies, to create forecasts for the blockchain expenditure in the 28 EU Member States. Delphi participants estimated blockchain expenditure of between €10.06 billion and €10.98 billion in 2030. Participants also estimated there would be up

to 102 million blockchain supported smart contract intra-EU transactions for goods in 2030.

Guidelines from the European Commission Better Regulation Toolbox were followed to develop cost benefit methods to examine the impact of policy options. Research also used relevant DG CONNECT Impact Assessments since 2017 (that had been positively received by the Regulatory Scrutiny Board) to provide robust insights to policy implementation expected impacts and costs. Timescales for policy implementation were found by examining policy implementation timelines for previous legislation associated with Connected Digital Single Market activities. Implementation generally took between one and two years.

Three of the four policy options proposed for '*legal issues regarding blockchain technology in general'* in the previous chapter are 'wait and see' options. Regulatory guidance is suggested to address the tension between blockchain reality and legal reality. Guidance, to be led by the European Commission, but with input from Member State governments, industry groups and other stakeholders is estimated to take one or two years to implement. Implementation of the guidance option is estimated to be €210,900 for one year of implementation and €421,800 for implementation over two years.

The impact of these policy options was investigated by examining changes in expenditure on blockchain. The proposed policies were expected to have between a two and three per cent impact per annum on blockchain expenditure across all 28 Member States. The baseline model predicted expenditure of €10.06 billion in 2030. A two per cent per annum increase in expenditure resulting from the policy option was estimated to increase the expenditure figure to €10.68 billion per annum in 2030, after taking account of the declining impact of policy during the ten year implementation period (called policy decay). Using the same methodology, a three per cent increase in expenditure resulting from the policy option was estimated to increase the expenditure €11.00 billion per annum in 2030. The impact of policy over the ten year time horizon will be cumulative. Cumulative estimates for impact are €2.89 billion for the forecast two per cent per annum increase and €4.38 billion for a three per cent increase due to the policy option.

Two of the nine policy options proposed for '*legal issues regarding smart contracts'* advocate the development of guidance. The remaining seven options are 'wait and see'. Like the preceding policy area, implementation of guidance is estimated to be €210,900 for one-year implementation and €421,800 for implementation over two years.

Additionally, similarly to the previous option, the impact of guidance policies is investigated at levels of two and three per cent per annum. At the lower impact level (two per cent), the impact of smart contracts on intra-EU trade would lead to cumulative transaction savings between 2022 and 2030 of €160 million. If the impact of guidance was three per cent, cumulative savings increase to €242 million.

Difficulties, highlighted at the workshop, in defining a *'utility token'* and in providing functional and legal criteria for utility tokens made it impossible to find relevant forecasts in the public domain. It was also noted that tokens can take on a hybrid nature overlapping with financial tokens. With this fluidity in definitions and parameters, it was not possible to develop a relevant and robust baseline model against which to estimate policy impacts.

Policy options for utility tokens are the only area in which the introduction of secondary legislation is envisaged. The development of secondary legislation for a previous

Directive estimated implementation costs of €4.7 million. This was therefore used as the guideline price for secondary legislation in this area. Three policy guidance options were also proposed. Implementation costs for these follow the previous rubric. Total policy option implementation costs in this area are estimated to be €4.922 million over a two to five year period.

It is evident from the above policy implementation costs estimates and impacts on baseline models that the benefits of the policy options hugely outweigh costs. Adopting the lowest impact predictions and highest policy option implementation costs, the benefits outweigh policy costs more than 500 times and this excludes any benefits arising from utility token options.

7. Conclusion

The report first introduces the technical, economic and governance context applicable to blockchain technology. With regard to the technical context, the report explains what blockchain technology constitutes exactly, and covers the varieties of blockchain as well as transaction capacities, environmental concerns, and cybersecurity. Moreover, the issues of integration with legacy systems, interoperability and standardisation, tokenisation as a means to provide incentives, and organisation and governance aspects are explored. After setting out this context, the report discusses a number of general legal issues in relation to blockchain technology. Hereafter, the different policy options available to the European Commission which could be considered to address the frictions identified are explained. More specifically, the options of wait-and-see, issuing of guidance and new supranational secondary legislation, as well as opt-in regimes and regulatory sandboxes are introduced and their advantages and disadvantages analysed. Combining the insights gathered, policy options that could remedy the legal issues that are described in relation to blockchain technology in general, smart contracts and utility tokens are then provided. Following this legal assessment, the report analyses the socio-economic impacts of blockchains and these policy options. Below, a short overview of the policy options suggested by the report and the economic impact of these options is provided.

Blockchain technology
With regard to blockchain technology, the report first looks at the issue of responsibility for legal compliance and liability. In terms of policy options, we consider that no specific policy response is needed and recommend that the European Commission adopt a wait-and-see approach. Furthermore, the Commission could incentivise industry efforts in relation to improved technical design that could enhance compliance. Lastly, stricter law enforcement by relevant national and supranational agencies would underline that compliance is not optional and create incentives of compliance for industry.

Secondly, the report considers potential barriers in sectoral legislation and the potential impact of DLT on data retention rules, such as those arising under the Anti Money-Laundering Directive. A possible policy option provided in this regard is for the Commission to adopt a wait-and-see approach. Should the Commission wish to adopt a more active approach, it could proactively encourage that blockchain-based AML systems are designed in order to ensure compliance with existing regulation from a technical perspective such as through research funding. Lastly, the adoption of standards terms and conditions or contracts could be used to coordinate compliance.

Thirdly, since DLT can also be used to infringe fundamental legal principles or mandatory rules and it can be difficult to remove related content from the database, the protection of fundamental legal principles and mandatory rules are examined. The report finds that there is no immediate need for a concrete policy action and the European Commission should adopt a wait-and-see approach.

The fourth topic discussed in the report is that of the tension between blockchain reality and legal reality. In this regard, we recommend the adoption of a wait-and-see approach. Should the European Commission nonetheless want to adopt a more proactive approach, it could encourage the development of technical and governance solutions that are aimed at aligning on-chain and off-chain information (such as guidance on best practices) and provide research funding for projects seeking to address such issues.

In terms of the economic impact assessment, three of the four policy options proposed are thus 'wait and see' options. Regulatory guidance is suggested to address the tension between blockchain reality and legal reality. This is estimated to take one or two years to implement. Implementation of the guidance option is estimated to be €210,900 for one year of implementation and €421,800 for implementation over two years. The impact of these policy options was investigated by examining changes in expenditure on blockchain. The proposed policies were expected to have between a two and three per cent impact per annum on blockchain expenditure across all 28 Member States. The baseline model predicted expenditure of €10.06 billion in 2030. A two per cent per annum increase in expenditure resulting from the policy option was estimated to increase the expenditure figure to €10.68 billion per annum in 2030, after taking account of the declining impact of policy during the ten year implementation period (called policy decay). Using the same methodology, a three per cent increase in expenditure resulting from the policy option was estimated to increase the expenditure €11.00 billion per annum in 2030. The impact of policy over the ten year time horizon will be cumulative. Cumulative estimates for impact are €2.89 billion for the forecast two per cent per annum increase and €4.38 billion for a three per cent increase due to the policy option.

Smart contracts
With regard to smart contracts, the report starts by examining the application of contract law. Here, it has been observed that contract law applies to smart contracts provided that these indeed qualify as legal contracts. Thus, no specific action needs to be taken at this stage. However, the Commission could issue regulatory guidance on the specific case of cross-border transactions (it may be that a contract valid in one jurisdiction is not valid in another).

Next, the national legal requirements on the need for a written form of the contract are considered. In this regard, it was recommended that the Commission adopt a wait-and-see approach.

Thirdly, the application of consumer law to smart contracts is discussed. The report finds that the Commission could adopt a wait-and-see approach. Moreover, the Commission could engage a discussion on the specific issue of the right to withdrawal under the Consumer Rights Directive and could also choose to adopt regulatory guidance on how precisely consumer protection law applies to smart contracts.

Following this, the issue of smart contracts and pseudonymity is examined, and the report finds that the Commission could encourage the adoption of standard contractual clauses related to the identification of parties that could be used by actors wishing to use blockchains. Beyond this, the Commission could also monitor the issue, and if considered appropriate, encourage the development of digital and/or SSI systems, such as for instance through research funding.

The fifth issue evaluated is that of smart contracts and jurisdiction, and it is found that the adoption of a wait-and-see approach seems well-suited in this domain.

Next, the issue of the capacity to contract and the protection of minors is assessed. Again, there does not appear to be an immediate need for regulatory intervention in the domain. The Commission could, however, provide research funding for projects seeking to provide innovative solutions.

The seventh area of examination is that of opacity. It deals with the questions of how parties without the necessary technical background can negotiate, draft and adjudicate

smart contracts. In this regard, the report suggests the Commission could adopt a wait-and-see approach, as well as possibly encouraging related research funding for projects.

Following this, smart contract arbitration mechanisms and in particular the question of the compatibility between smart contract arbitration mechanisms and legal requirements regarding arbitration proceedings is assessed. It is concluded that a wait-and-see approach could provide further clarity on the question of whether requirements to file documents in national courts merely seek to achieve public policy objectives in a technology-neutral manner or whether they might unduly limit the development of smart contract arbitration mechanisms in the EU. The Commission could, however, also encourage the adoption of standard arbitration clauses to assist and help businesses in this regard.

Finally, the potential impact of smart contracts on notarisation was looked at. Many have argued that DLT could facilitate the notarial profession's task due to its tamper-resistance and possibility of coordination through multiple parties. It is, however, sometimes feared that legal requirements around notarisation could prevent digital transactions from being concluded purely through digital means. We recommend that the European Commission continues to monitor developments in this area.

Assessing the impacts of the above, two of the nine policy options proposed thus advocate the development of guidance. The remaining seven options are 'wait and see'. Like the preceding policy area, implementation of guidance is estimated to be €210,900 for one year implementation and €421,800 for implementation over two years. Additionally, similarly to the previous option, the impact of guidance policies is investigated at levels of two and three per cent per annum. At the lower impact level (two per cent), the impact of smart contracts on intra-EU trade would lead to cumulative transaction savings between 2022 and 2030 of €160 million. If the impact of guidance was three per cent, impact cumulative savings increase to €242 million.

Utility tokens
In relation to utility tokens, the lack of legal certainty and regulatory fragmentation is covered in detail. Our analysis concerning this topic found that European regulators could either reduce uncertainty and fragmentation through the issuing of regulatory guidance as to how related legal frameworks apply to utility tokens or consider the creation of a supranational regime on utility tokens.

Secondly, the application of consumer protection law as well as prospectus requirements to utility tokens as examined. The report finds that in this respect, the Commission could encourage the adoption of standards by industry that may subsequently be endorsed by regulation, and that guidance by the European Commission and/or national authorities regarding how precisely consumer protection law applies to utility tokens may be adopted.

Finally, trading on secondary markets is discussed. To address this matter, the Commission could adopt regulatory guidance on the rules applicable in case utility tokens are traded on secondary markets and encourage the adoption of standards by industry which are subsequently endorsed by regulation if need be.

Concerning the economic impact, difficulties in defining a *'utility token'* and in providing functional and legal criteria for utility tokens made it impossible to find relevant forecasts in the public domain. With this fluidity in definitions and parameters, it was not possible to develop a relevant and robust baseline model against which to estimate policy impacts. Policy options for utility tokens are the only area in which the introduction of secondary legislation is envisaged. The development of secondary legislation for a

previous Directive estimated implementation costs of €4.7 million. This was therefore used as the guideline price for secondary legislation in this area. Three policy guidance options were also proposed. Implementation costs for these follow the previous rubric. Total policy option implementation costs in this area are estimated to be €4.922 million over a two to five year period.

Annex I - Bibliography

Below, please find the sources of literature which were reviewed.

Books

- Armstrong J, 'Principles of Forecasting: A Handbook for Researchers and Practitioners' (2002), International Series in Operations Research & Management Science, Springer Science.
- Barner R., 'Team Troubleshooter: How to Find and Fix Team Problems' (2000), Davies-Black.
- Bartoletti M. and Pompianu L., 'An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns' in Michael Brenner et al (eds), Financial Cryptography and Data Security (Springer 2017).
- Belli L., Francisco P.A and Zingales N., 'Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police' in Luca Belli and Nicolo Zingales (eds), Platform regulations: how platforms are regulated and how they regulate us (FGV Direito Rio 2017).
- Burke Johnson R. and Christensen L., 'Quantitative, Qualitative, and Mixed Research Approaches' (2014), Sage, p.427 – 448.
- Dixon P. , 'Futurewise: The Six Faces of Global Change' (2007), Profile Books.
- Fisher JC and Pry R, 'A simple substitution model for technological change'(1971), Technological forecasting and social change, n°3, p.75-88.
- Foley P. and Masser I, 'Expert opinion and urban analysis Urban Studies (1987),24, p.217 – 225.
- Idelberger F. et al, 'Evaluation of Logic-Based Smart Contracts for Blockchain Systems' in Jose Julia Alferes et al (eds), Rule Technologies. Research, Tools, and Applications (Springer 2016).
- Porter I, Cunningham S, Banks J, Roper T, Mason T and Rossini F, 'Forecasting and management of technology (1991), John Wiles and Sons, p.138-145.
- Reyes C., 'Moving Beyond Bitcoin to an Endogenous Theory of Decentralised Ledger Technology Regulation: An Initial Proposal' (2016), vol.61, Villanova Law Review 191.
- Rühl G., Bartoletti M. and Pompianu L., 'An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns' in Michael Brenner et al (eds), Financial Cryptography and Data Security (Springer 2017).
- Schulz W. and Held t., 'Regulated Self-Regulation as a Form of Modern Government'(2004),John Libbey Publishing.

Articles

- Borgogno O., 'Smart Contracts as the (new) Power of the Powerless? The Stakes for Consumers' (2018) Vol. 26, European Review of Private Law, Issue 6, 885-902.
- Cutts T., 'Smart Contracts and Consumers', LSE Working Papers, April 2019.
- De Filippi P. and Wright A., 'Blockchain and the Law: the Rule of Code' (2018), Harvard University Press, available at https://www.hup.harvard.edu/catalog.php?isbn=9780674976429.
- Engelhardt M., 'An introduction to blockchain technology in the healthcare sector (2017)', Technology Innovation Management Review, vol. 7, n°10. P.22 -34.
- Finck M., 'Blockchains and the GDPR' (2018), 4 European Data Protection Law Review, p.17-35.
- Finck M., 'Blockchains Regulating the Unknown' (July 2018), German Law Journal, vol.19, issue 4.

- Finck M., Blockchain Regulation and Governance in Europe, Cambridge University Press (December 2018).
- Freedman D., 'Statistical Models: Theory and Practice' (2009), Cambridge University Press.
- Flyvbjerg B., Skamris M. Holm, and Buhl S., 'Underestimating Costs in Public Works Projects: Error or Lie?'(2002), Journal of the American Planning Association, vol. 68, n°3, p.279-295.
- Melchior E., 'Réflexions juridiques autour de la blockchain: analyse sous l'angle du droit des contrats' (2019) 72, Revue du droit des technologies de l'information, n° 45.
- Marsden C., 'Internet Co-Regulation' (2011), Cambridge University Press.
- Narayanan A. et al, 'Bitcoin and Cryptocurrency Technologies' (2016), Princeton University Press.
- Narayanan A. and Clark J., 'Bitcoin's academic pedigree' (2017), Communications of the ACM, Vol. 60, No. 12, Pages 36-45.
- Tan Cheng Han, SC, Walter Woon on Company Law, (Sweet & Maxwell, Revised 3rd Ed, 2009), p.85–86.
- Walch A. ,' In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains'(2018), in Georgios Dimitropoulos et al (eds), The Blockchain Revolution: Legal & Policy Challenges, Oxford University Press.
- Yermack D., 'Corporate Governance and Blockchains' (2017), 21 Review of Finance 7.

Online sources

- 'An Introduction to DAGs and How They Differ From Blockchains' (June 2018), https://medium.com/fantomfoundation/an-introduction-to-dags-and-how-they-differ-from-blockchains-a6f703462090.
- 'An Overview of Comos Hub Governance' (March 2019), https://blog.chorus.one/an-overview-of-cosmos-hub-governance/.
- 'Annoucing the Kusama Network' (July 2019), https://polkadot.network/kusama-network-the-canary-network/.
- 'AXA goes blockchain with fizzy' (13 September 2017), https://www.axa.com/fr/newsroom/actualites/axa-se-lance-sur-la-blockchain-avec-fizzy.
- 'Blockchain: Impacts on Notarial Professions' (Oct 2019), https://hackernoon.com/blockchain-impacts-on-notarial-professions-a58245030a3f.
- 'Blockchain and the General Data Protection Regulation' (July 2019), https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2019)634445.
- 'Blockchain and the notaries: the services won't be replaced but transformed' (August 2018), https://www.fintechfutures.com/2018/08/blockchain-and-the-notaries-the-services-wont-be-replaced-but-transformed/.
- 'Blockchain challenges and opportunities: A survey, International Journal of Web and grid Services' (October 2018), available at https://www.researchgate.net/publication/328338366_Blockchain_challenges_and_opportunities_A_survey/link/5bd1e50d299bf12253b018d9/download.
- 1_Beitrag_Fusswinkel_en.html;jsessionid=AA4F226A1806115F3FC4AD10BCB21307.1_cid390?
- 'Blockchain-Strategie der Bundesregierung', available at https://www.bundesfinanzministerium.de/Content/DE/Pressemitteilungen/Finanzpolitik/2019/09/2019-09-18-PM-Block-Anlage.pdf?__blob=publicationFile&v=6.
- 'Blockchain-Technologie' (June 2017), available at https://www.bafin.de/DE/Aufsicht/FinTech/Blockchain/blockchain_artikel.html.

- 'Blokchain Technology-Thoughts on Regulation' (Aug 2018) https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/BaFinPerspektiven/2018/bp_18-1_Beitrag_Fusswinkel_en.html;jsessionid=AA4F226A1806115F3FC4AD10BCB21307.1_cid390.
- 'Can the interoperability of blockchains change the world?' (Feb 2019) https://www.capgemini.com/2019/02/can-the-interoperability-of-blockchains-change-the-world/.
- 'Crypto tokens remain a risk for consumers', https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2019/fa_bj_1902_kryptowaehrung_en.html.
- 'CSA Regulatory Sandbox' http://www.iam-media.com/reports/detail.aspx?g=ccb604f5-1194-4d8d-89c0-cc44306f74da.
- 'Efforts = effects? Blockchain standardisation overview', https://savangard.com/en/2018/08/22/blockchain-standardisation-efforts-overview/.
- 'Finma publishes ICO guidelines' (Feb 2018), https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/.
- 'FINMA reduces obstacles to FinTech' (17 March 2016) https://www.finma.ch/en/news/2016/03/20160317-mm-fintech/.
- 'FinTech Regulatory Sandbox: Introduction', http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/FinTech-Regulatory-Sandbox.aspx.
- 'Fintech Supervisory Sandbox', http://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech-supervisory-sandbox.shtml.
- 'ICO selects first participants for data protection Sandbox' (July 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-selects-first-participants-for-data-protection-sandbox/.
- 'Initial coin offerings: High risks for consumers' (Nov 2017), https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2017/fa_bj_1711_ICO_en.html.
- 'Investor Bulletin: initial Coin Offerings' (July 2017), https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings.
- 'Koalitionsvertrag zwischen CDU, CSU und SPD' (12 March 2018), n°124, available at https://www.cdu.de/system/tdf/media/dokumente/koalitionsvertrag_2018.pdf?file=1.
- 'Mining Bitcoin uses More Energy than Denmark Study' (Nov 2018), https://www.thelocal.dk/20181106/mining-Bitcoin-uses-more-energy-than-denmark-study.
- 'More room for innovation in the financial sector' (Dec 2016) https://www.dnb.nl/en/binaries/More-room-for-innovation-in-the-financial%20sector_tcm47-361364.pdf?2018050113.
- 'Notarization in Blockchain: Part 1' (Aug 2018), https://medium.com/@kctheservant/notarization-in-blockchain-part-1-a9795f19e28d.
- 'Notarization in Blockchain', https://www.blockchainexpert.uk/blog/notarization-in-blockchain.
- 'Security 'Secure Hashing: Approved Algorythms', https://web.archive.org/web/20110625054822/http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html.
- 'Smart Contracts: Rechtliche Voraussetzungen und Herausforderungen' (Smart Contracts: Legal requirements and challenges), https://www.srd-rechtsanwaelte.de/blog/smart-contracts-recht.

- 'The legislative train schedule for the Connected Digital Single Market', http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-5g-action-plan.
- 'Unlocking the blockchain: a global legal and regulatory guide', available at https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/imported/unlocking-the-blockchain---chapter-1.pdf.
- 'Why is Blockchain A Good Solution for KYC Verification', https://www.devteam.space/blog/why-is-blockchain-a-good-solution-for-kyc-verification/.
- 'Worldwide Spending on Blockchain Forecast to Reach $11.7 Billion in 2022, According to New IDC Spending Guide' (July 2018), available at https://www.idc.com/getdoc.jsp?containerId=prUS44150518.
- 'Google processes 40k searches per second', https://www.quora.com/Google-processes-40k-searches-per-second-On-average-a-web-server-can-handle-1000-requests-per-second-Does-that-mean-Google-can-run-using-only-40-web-servers.
- Aaron von Wirdum, 'A primer on Bitcoin Governance, or Why Developers Aren't in Charge of the Protocol', https://bitcoinmagazine.com/articles/a-primer-on-bitcoin-governance-or-why-developers-aren-t-in-charge-of-the-protocol-1473270427.
- Accenture-Clearstream, 'Collateral Management – Unlocking the Potential in Collateral' (2011), available at https://www.clearstream.com/resource/blob/1316326/e5bf3b589c8f3ff6afd19166f9d53d3b/accenture-collateral-report-pdf-data.pdf.
- Adam Barone 'The future of Cryptocurrency in 2019 and beyond' available at https://www.investopedia.com/articles/forex/091013/future-cryptocurrency.asp.
- Agrawal H, 'What are security tokens and why is the market bullish' (2019), available at https://coinsutra.com/security-tokens/.
- Alexander F. Wagner, Rolf H. Weber, 'Corporate Governance auf der Blockchain', SZW/RSDA, 1/2017, available at https://www.uzh.ch/dam/bf/persons/employee-assets/wagner_alexander/papers/SZW_1_2017_Wagner_Weber_Published.pdf.
- Allen & Overy, 'Legal and Regulatory risks for the finance sector: Cryptocurrency AML risk considerations', http://www.allenovery.com/publications/en-gb/lrrfs/cross-border/Pages/Cryptocurrency-AML-risk-considerations.aspx.
- Allens, 'Blockchain reaction: understanding the opportunities and navigating the legal frameworks of distributed ledger technology and blockchain' available at https://www.allens.com.au/globalassets/pdfs/specials/blockchainreport.pdf.
- Alon Gal, 'The Tangle: an illustrated Introduction' (Jan 2018), https://blog.io.ta.org/the-tangle-an-illustrated-introduction-4d5eae6fe8d4.
- Alyssa Hertig, 'Bitcoin's Dropping Lightning Capacity Might not Be a Bad Thing' (October 2019), https://www.coindesk.com/bitcoins-dropping-lightning-capacity-might-not-be-a-bad-thing.
- AMF, 'Vers un nouveau régime pour les crypto-actifs en France' (April 2019), https://www.amf-france.org/Reglementation/Dossiers-thematiques/Fintech/Vers-un-nouveau-regime-pour-les-crypto-actifs-en-France.
- Amy Cortese, 'Blockchain Technology Ushers in "The Internet of Value', (Cisco,10 February 2016), available at https://newsroom.cisco.com/feature-content?articleId=1741667.
- Ana Alexandre, 'Walmart is ready to use blockchain for its live food business' (April 2018), https://cointelegraph.com/news/walmart-is-ready-to-use-blockchain-for-its-live-food-business.
- Anatoly Yakovenko, 'Proof of History: a clock for blockchain' (April 2018), https://medium.com/solana-labs/proof-of-history-a-clock-for-blockchain-cf47a61a9274.
- Andrew Tobyn, 'Sovrin What Goes on the Ledger?' (Sept 2018), available on https://www.evernym.com/wp-content/uploads/2017/07/What-Goes-On-The-Ledger.pdf.

- Angela Walch, 'Deconstructing 'Decentralization: Exploring the core Claim of Crypto Systems' (Feb 2019), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3326244.
- Angela Walch, 'The Path of the Blockchain Lexicon (and the Law)' (March 24, 2017), 36 Review of Banking & Financial Law 713 (2017). Available at SSRN: https://ssrn.com/abstract=2940335.
- Ari Juels, Ahmed Kosba, Elaine Shi, 'The Ring of Gyges: Using Smart Contracts for Crime', available at http://www.arijuels.com/wp-content/uploads/2013/09/Gyges.pdf.
- Armstrong J S, 'Forecasting standards checklist' (2001), available at http://www.forecastingprinciples.com/files/pdf/Armstrong_2001_Checklist.pdf.
- Armstrong S and Green K, 'Forecasting methods and principles: Evidence based checklists' (2018), Journal of Global Scholars of Marketing Science. 28, p.2, available at https://www.tandfonline.com/doi/full/10.1080/21639159.2018.1441735.
- Bent Flyvbjerg, 'From Nobel Prize to Project Management: Getting Risks Right, Project Management Journal. Vol. 37, n° 3, p.5-15 available at http://arxiv.org/abs/1302.3642.
- Bitcoin Energy Consumption Index (2019), https://digiconomist.net/Bitcoin-energy-consumption.
- Body of European Regulators for Electronic Communications, https://berec.europa.eu/.
- Bryan Weinberg, 'Blockchain and KYC: Know Your Customer Better' (Jan 2019), https://openledger.info/insights/blockchain-kyc/.
- Buckey, Ross P. and Arner, Douglas W and Veidt, Robin and Zetsche, Dirk Andreas, 'Building FinTech Ecosystems: Regulatory Sandboxes, Innovation Hybs and Beyond' (September 2019), UNSX Law Research paper No.19-72, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3455872.
- Chamber of Digital Commerce, 'Smart contracts: Is the Law Ready?' (Sept 2018), https://digitalchamber.org/smart-contracts-whitepaper/.
- Charles McLellan, 'Analysing the analysts: Predicting emerging technologies' (2014), http://www.zdnet.com/article/analysing-the-analysts-predicting-emerging-technologies.
- Chetcuchi Cauchi Advocates, 'Malta Utility Token Offering', https://www.ccmalta.com/malta-utility-token-offering.
- Chief Economist Note, 'How important are EU exports for jobs in the EU?' (Nov 2018), available at http://trade.ec.europa.eu/doclib/docs/2018/november/tradoc_157517.pdf.
- Christian Catalini and Joshua S. Gans, Some Simple Economics of the Blockchain (April 20, 2019). Rotman School of Management Working Paper No. 2874598; MIT Sloan Research Paper No. 5191-16, available at SSRN: https://ssrn.com/abstract=2874598 or http://dx.doi.org/10.2139/ssrn.2874598.
- Christina Majaski, 'Security token definition' (2019), https://www.investopedia.com/terms/s/security-token.asp.
- Christopher Koopman et al, 'The Sharing Economy and Consumer Protection Regulation: The Case for Policy Change' (2014), https://www.mercatus.org/publication/sharing-economy-and-consumer-protection-regulation-case-policy-change.
- Clifford Chance and European Bank for Reconstruction and Development, 'Smart Contracts – Legal Framework and Proposed Guidelines for Lawmakers' (September 2018), available at: www.ebrd.com/documents/pdf-smart-contracts-legal-framework-and-proposed-guidelines-for-lawmakers.pdf.

- Consensys, 'Blockchain for government and the public sector' (2019), https://consensys.net/enterprise-ethereum/use-cases/government-and-the-public-sector/.
- Consensys, 'The Roadmap to Serenity' (2016), https://media.consensys.net/the-roadmap-to-serenity-bc25d5807268.
- Consiglio nazionale del notario, 'Il notario presenta "Notarchain", la Blockchain certificata dei notai e i registri volontari digitali' (Oct 2017), available at https://www.notariato.it/sites/default/files/cs_notarchain_13102017.pdf.
- CONSOB, 'Initial Coin Offerings and Crypto-Assets Exchanges, Call for Evidence' (19 March 2019), available at http://www.consob.it/documents/46180/46181/doc_disc_20190319_en.pdf/e981f8a9-e370-4456-8f67-111e460610f0.
- Credentials Community Group, 'A Primer for Decentralized Identifiers', Draft Community Report (19 Jan 2019), available at https://w3c-ccg.github.io/did-primer/.
- Darcy Allen, Alastair Berg, Chris Berg, Brendan Markey-Towler, and Jason Potts, 'Some Economic Consequences of the GDPR' (March 29, 2019), Economics Bulletin, vol. 39, no. 2, p.785-797, Available at SSRN: https://ssrn.com/abstract=3160404 or http://dx.doi.org/10.2139/ssrn.3160404.
- Dean Franklet et al., 'Public implementation of blockchain technology. Department of economics and finance' (2018), University of Canterbury, available at https://ir.canterbury.ac.nz/bitstream/handle/10092/16353/Department%20of%20Economics%20working%20paper%201823.pdf?sequence=2&isAllowed=y.
- Decentralized Key management', https://hyperledger-indy.readthedocs.io/projects/sdk/en/latest/docs/design/005-dkms/README.html.
- Deloitte and Fundsquare, 'Europe's funds expenses at a crossroads: The benefits of mutualising the cost of distribution' (2015), available at https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/IM/lu-en-europe-fund-expenses-survey-24062015.pdf
- Deloitte, "Blockchain and Cybersecurity. Let's discuss", available at https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf.
- Deloitte, 'Blockchain: Legal implications, questions, opportunities and risks' (2018), https://www2.deloitte.com/global/en/pages/legal/articles/2018-legal-blockchain.html.
- Deloitte, 'CFO Insights: Getting smart about smart contracts' (2016), https://www2.deloitte.com/tr/en/pages/finance/articles/cfo-insights-getting-smart-contracts.html.
- Dentons, 'Using blockchain for KYC/AML compliance' (May 2019), https://www.dentons.com/en/insights/articles/2019/may/28/using-blockchain-for-kyc-aml-compliance.
- Digital Chamber of Commerce, 'SMART CONTRACTS ALLIANCE, SMART CONTRACTS: Is the Law Ready?' (2018), available at https://lowellmilkeninstitute.law.ucla.edu/wp-content/uploads/2018/08/Smart-Contracts-Whitepaper.pdf.
- Djuri Baars, 'Towards self-sovereign identity using blockchain technology', Masters Thesis, University of Twente, available at http://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf.
- Douglas McWilliams , Cristian Marcu and Beatriz Cruz, 'The economic impact of smart ledgers on world trade'(2018), available at https://www.longfinance.net/media/documents/Economic_Impact_Of_Smart_Ledgers_On_World_Trade.pdf.
- Dr. Arati Baliga, 'Understanding Blockchain Consensus Models' (April 2017), available at

https://pdfs.semanticscholar.org/da8a/37b10bc1521a4d3de925d7ebc44bb606d740.pdf.
- Ed Felten, 'Blockchain: What is it good for?' (26 February 2018), available at https://freedom-to-tinker.com/2018/02/26/bloc.
- EDPB Workshop Program 2019/2020, available at https://edpb.europa.eu/our-work-tools/our-documents/work-program/edpb-work-program-20192020_en.
- EU Blockchain Forum and Observatory, 'Report on Legal and Regulatory Framework for Blockchains and Smart Contracts', available at https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf?width=1024&height=800&iframe=true.
- European Banking Authority (EBA), 'Report with advice for the European Commission on cryptoassets' (January 2019), available at https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf.
- European Banking Authority (EBA), 'Report with advice to European Commission on Cryptoassets' (Jan 2019), available at https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf?retry=1.
- European Commission, 'Better Regulation Toolbox' (July 2017), http://www.emcdda.europa.eu/document-library/better-regulation-toolbox-european-commission_en.
- European Commission, 'Commission Staff Working Document, Executive Summary of the Impact Assessment Accompanying the document Commission Regulation laying down Ecodesign requirements for servers and data storage products pursuant to Directive 2009/125/EC of the European Parliament and of the Council and amending Commission Regulation (EU) N°617/2013' (15 March 2019), available at https://ec.europa.eu/transparency/regdoc/rep/10102/2019/EN/SWD-2019-105-F1-EN-MAIN-PART-1.PDF.
- European Commission, 'Commission Staff Working Document, Impact Assessment Accompanying the document Proposal for a regulation of the European parliament and of the Council on establishing a single digital gateway to provide information, procedures, assistance and problem solving services and amending Regulation (EU) No 1024/2012' (2 May 2017), available at https://ec.europa.eu/transparency/regdoc/rep/10102/2017/EN/SWD-2017-213-F1-EN-MAIN-PART-3.PDF.
- European Commission, 'Interinstitutional Agreement on Better Law-Making' [2003,] OJ, C 321/01, 31.12.2003, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32003Q1231%2801%29.
- European Commission salaries, https://www.glassdoor.co.uk/Salary/European-Commission-Brussels-Salaries-EI_IE147109.0,19_IL.20,28_IM992.htm.
- European Union Blockchain Observatory & Forum, 'Key challenges and barriers for blockchain in the European Union' in Blockchain Innovation in Europe Report (August 2018), available at https://www.eublockchainforum.eu/sites/default/files/reports/20180727_report_innovation_in_europe_light.pdf?width=1024&height=800&iframe=true.
- European Union Blockchain Observatory and Forum, Report on "Blockchain and digital identity", available at https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf.
- European Parliament, 'Resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation' (2017/2772(RSP)), B8-0397/2018, https://www.europarl.europa.eu/doceo/document/B-8-2018-0397_EN.html.
- European Parliament, 'Making the Most of Globalization: EU Trade Policy explained' (June 2019),

https://www.europarl.europa.eu/news/en/headlines/economy/20190528STO53303/making-the-most-of-globalisation-eu-trade-policy-explained.
- Eurostat, 'The EU in the world: International trade' (2018), available at https://ec.europa.eu/eurostat/statistics-explained/pdfscache/20442.pdf.
- Eurostat, Mean annual earnings by sex, age and occupation - NACE Rev. 2, [earn_ses14_28] €43,777 (2020), available at http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=earn_ses14_28&lang=en.
- EY, Global Banking Outlook (2018), available at https://www.ey.com/Publication/vwLUAssets/ey-global-banking-outlook-2018/$File/ey-global-banking-outlook-2018.pdf.
- FCA, 'Regulatory Sandbox', https://www.fca.org.uk/firms/regulatory-sandbox.
- Filippo Annunziata, 'Speak If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offerings' (February 11, 2019). Bocconi Legal Studies Research Paper No. 2636561. Available at SSRN: https://ssrn.com/abstract=3332485 or http://dx.doi.org/10.2139/ssrn.3332485.
- Finma, 'Guidance 02/2019: Payments on the blockchain' (August 2019), available at https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20190826-finma-aufsichtsmitteilung-02-2019.pdf?la=en.
- Finma, 'Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs) (Feb 2018), available at https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en.
- Forbes, 'Blockchains value isn't currency, It's technology' (July 2015), https://www.forbes.com/sites/robertrosenkranz/2015/07/07/bitcoins-value-isnt-currency-its-technology/#6bb33fe11f11.
- Garrick Hilleman and Michel Rauchs, 'Global cryptocurrency benchmarking Study' (2017), available at https://www.researchgate.net/publication/317059599_2017_Global_Cryptocurrency_Benchmarking_Study.
- Giesela Rühl, 'The Law applicable to smart contracts, or much ado about nothing?' (Jan 2019), available at https://www.law.ox.ac.uk/business-law-blog/blog/2019/01/law-applicable-smart-contracts-or-much-ado-about-nothing.
- Global Legal Monitor, 'Malta: Government Passes Three Laws to Encourage blockchain Technology' https://www.loc.gov/law/foreign-news/article/malta-government-passes-three-laws-to-encourage-blockchain-technology/.
- 'Liechtenstein preparing Blockchain Act' (August 2018) https://www.liechtenstein.li/en/news-detail/article/liechtenstein-preparing-blockchain-act/.
- Gunjan Bhardwaj, 'Can blockchain solve pharma's counterfeit drug problem?' (April 2018), https://pharmaphorum.com/views-and-analysis/can-blockchain-solve-pharmas-counterfeit-drug-problem/.
- Hbar Economics, 'A deep dive into the dual rôle of Hbars and detailed release schedule', https://www.hedera.com/hh-hbar-coin-economics-paper-100919-v2.pdf.
- IBM, 'Emerging technology projection: The total economic impact of IBM blockchain: Projected Cost Savings And Business Benefits Enabled By IBM Blockchain' (July 2018), available at https://www.ibm.com/downloads/cas/QJ4XA0MD.
- IDC, Worldwide Semiannual Blockchain Spending Guide (2019), available at https://www.idc.com/getdoc.jsp?containerId=IDC_P37345.
- 'Initial Coin Offering: Note on the Classification of Tokens as Financial Instruments', Ref. No. W A 11-QB 4100-2017/0010 (March 28, 2018),

https://www.bafin.de/SharedDocs/Downloads/EN/Merkblatt/WA/dl_hinweisschreiben_einordnung_ICOs_en.html.

- Jake Goldenfein and Andrea Leiter, 'Legal Engineering on the Blockchain: "Smart Contracts" as Legal Conduct' (2018) Law and Critique (Forthcoming), available at SSRN: https://ssrn.com/abstract=3176363.
- James Martin, 'Lost on the Silk Road: Online drug distribution and the 'cryptomarket'' (October 2013) available at https://journals.sagepub.com/doi/abs/10.1177/1748895813505234.
- James Ray, 'Sharding Roadmap', https://github.com/ethereum/wiki/wiki/Sharding-roadmap#strongphase-1strong-basic-sharding-without-evm.
- James Vincent, 'Bitcoin consumes more energy than Switzerland, according to new estimate' (2019), https://www.theverge.com/2019/7/4/20682109/Bitcoin-energy-consumption-annual-calculation-cambridge-index-cbeci-country-comparison.
- Jared R. Butcher, Steptoe & Johnson LLP, and Claire M. Blakey, Paul Hastings LLP, with Practical Law Data Privacy Advisor, Practical Law, 'Cybersecurity Tech Basics: Blockchain Technology Cyber Risks and Issues: Overview' , available at https://www.steptoe.com/images/content/1/8/v2/189187/Cybersecurity-Tech-Basics-Blockchain-Technology-Cyber-Risks-and.pdf.
- Jibrel Network, 'Coins vs. Tokens - The Complete Guide', https://jibrel.network/en/blog/blockchain/token-vs-coin/.
- Joel Camacho, 'Utility tokens: A general understanding' (2018), https://medium.com/coinmonks/utility-tokens-a-general-understanding-f6a5f9699cc0.
- John Bohannon, 'Why criminals can't hide behind Bitcoin' (March 2016), https://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin.
- JonesDay, 'ICOs and Token Regulation from a German Perspective' (Oct 2018) https://www.jonesday.com/en/insights/2018/10/icos-and-token-regulation-from-a-german-perspective.
- Jose Parra-Moyano, Omri Ross, 'KYC Optimization Using Distributed Ledger Technology' (Jan 2017), available at https://www.researchgate.net/publication/315046134_KYC_Optimization_Using_Distributed_Ledger_Technology.
- Josh Swihart, Benjamin Winston and Sean Bowe, 'Zcash Counterfeiting Vulnerability Successfully Remediated' (Feb 2019), https://electriccoin.co/blog/zcash-counterfeiting-vulnerability-successfully-remediated/.
- Julia Black, 'Constitutionalising Self-Regulation' (Jan 1996) 59, Modern Law Review, p.24, available at https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1468-2230.1996.tb02064.
- Julia Black, 'Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a "Post-Regulatory" World' (Feb 2001), 54 Current Legal Problems 103, available at https://www.researchgate.net/publication/30527050_Decentring_Regulation_Understanding_the_Role_of_Regulation_and_Self-Regulation_in_a_'Post-Regulatory'_World.
- Julie Maupin, 'The G20 countries should engage with blockchain technologies to build an inclusive, transparent, and accountable digital economy for all' (2017), Economics Discussion Papers, No. 2017-48, Kiel Institute for the World Economy (IfW), Kiel., available at http://hdl.handle.net/10419/163569.
- Karen Yeung, (Regulations by Blockchain: the Emerging Battle for Supremacy between the Code of Law and Code as Law' (March 2019), available at https://onlinelibrary.wiley.com/doi/10.1111/1468-2230.12399.
- Kevin Werbach & Nicolas Cornell, 'Contracts Ex Machina' (n 142), available at https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3913&context=dlj.

- Kim K and Kang T., 'Does technology against corruption always lead to benefit? The potential risks and challenges of blockchain technology', OECD Global anti-corruption and integrity forum,' available at https://www.oecd.org/cleangovbiz/Integrity-Forum-2017-Kim-Kang-blockchain-technology.pdf.
- Klint Finley, 'a $50 Million Hack Just Showed That the DAP was All too Human' (June 2016), https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/.
- Kyle Torpey, 'Bitcoin Mining Centralization is 'Quite Alarming', But A solution is in the Works' (July 2019) https://www.forbes.com/sites/ktorpey/2019/07/28/bitcoin-mining-centralization-is-quite-alarming-but-a-solution-is-in-the-works/#25e5c6d1530b.
- L. McKnight, 'Over the virtual top: Digital service value chain disintermediation', 42nd TPRC Research Conference on Communication, Information and Internet Policy George Mason University School of Law, Arlington, VA September 12th 2014, https://www.researchgate.net/publication/265599051_Over_the_Virtual_Top_Digital_Service_Value_Chain_Disintermediation_Implications_for_Hybrid_Hetnet_Regulation.
- Lauren Coleman, 'Here's why interest in tokenising assets is starting to surge' (2019), https://www.forbes.com/sites/laurencoleman/2019/04/25/heres-why-interest-in-tokenizing-assets-is-starting-to-surge/#63cacb3840a5.
- Lawrence Vanston and Ray Hodges, Technology forecasting for telecommunications (2004), available at www.tfi.com/pubs/w/pdf/telektronikk_peer.pdf.
- Lisa Walker, 'This new carbon currency could make us more climate friendly' (2017), World Economic Forum Agenda blog, available at https://www.weforum.org/agenda/2017/09/carbon-currency-blockchain-poseidon-ecosphere.
- Luke Parker, 'European Commission "actively monitoring" Blockchain developments' (17 February 2017), https://bravenewcoin.com/insights/european-commission-actively-monitoring-blockchain-developments.
- M Demertzis, S Merler, G Wolff, 'Capital Markets Union and the fintech opportunity' (2018), available at http://www.guntramwolff.net/wp-content/uploads/2018/07/fintech.pdf.
- Mackenzie Garrity, 'Pharma companies consider blockchain to track counterfeit drugs' (2019), Hospital Review, https://www.beckershospitalreview.com/pharmacy/pharma-companies-consider-blockchain-to-track-counterfeit-drugs.html.
- Madeleine Cuff, 'Ben and Jerry's scoop blockchain pilot to serve up carbon-offset ice-cream' (2018), https://businessgreen.com/bg/news/3033147/ben-and-jerrys-scoop-blockchain-pilot-to-serve-up-carbon-offset-ice-cream.
- Maren K. Woebbeking, 'The Impact of Smart Contracts on Traditional Concepts of Contract Law'(2019), available at https://www.jipitec.eu/issues/jipitec-10-1-2019/4880.
- Mario Monti, 'A New Strategy for the Single Market – At the Service of Europe's Economy and Society', available at http://ec.europa.eu/bepa/pdf/monti_report_final_10_05_2010_en.pdf.
- Mark Giancaspro, 'Is a "smart contract" really a smart idea? Insights from a legal perspective' (2017), 33 Computer Law & Security Review, available at https://www.researchgate.net/publication/317354410_Is_a_'smart_contract'_really_a_smart_idea_Insights_from_a_legal_perspective.
- Mark Papermaster, 'Blokchains and Its Implementation Challenges' (April 2018) https://www.networkcomputing.com/network-security/blockchain-and-its-implementation-challenges.
- Markus Kaulartz, 'Smart Contract Dispute Resolution', in Martin Fries and Boris Paal (eds) 'Smart Contracts'(2019), Mohr Siebeck, available at https://www.mohrsiebeck.com/buch/smart-contracts-9783161569104.

- Martin Fries, 'Law and Autonomous Systems Series: Smart consumer contracts - The end of civil procedure?' (March 2018), Oxford Business Law Blog, available at https://www.law.ox.ac.uk/business-law-blog/blog/2018/03/smart-consumer-contracts-end-civil-procedure.
- Massimo Bartoletti and Livio Pompianu, 'An empirical analysis of smart contracts: Platforms, applications, and design patterns' (2017), in Michael Brenner et al (eds), Financial Cryptography and Data Security, Springer, available at https://www.springerprofessional.de/en/an-empirical-analysis-of-smart-contracts-platforms-applications-/15236404.
- Mateja Durovic and André Janssen, 'The Formation of Blockchain-Based Smart Contracts in the Light of Contract Law' (2018), European Review of Private Law, available at http://static.ie.edu.s3.amazonaws.com/Tertulia/Papers%202018/Papers/The%20Formation%20of%20Blockchain-based%20Smart%20Contracts%20in%20the.pdf.
- Mateja Durovic and André Janssen, 'The Formation of Blockchain-Based Smart Contracts in the Light of Contract Law' (2018), European Review of Private Law, available at http://static.ie.edu.s3.amazonaws.com/Tertulia/Papers%202018/Papers/The%20Formation%20of%20Blockchain-based%20Smart%20Contracts%20in%20the.pdf.
- Matthew Bedham, 'Three countries host over 50 per cent of world's Bitcoin nodes' (2019), https://thenextweb.com/hardfork/2019/02/27/3-countries-50-perecent-Bitcoin-network/.
- Matthias Mettler, 'Blockchain technology in healthcare: The revolution starts here', available at https://ieeexplore.ieee.org/abstract/document/7749510.
- McKinsey, ' Blockchain beyond the hype: What is the strategic business value? (2018), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value.
- Medium Corporation, 'Utility tokens: How they work and why they are so important' (2018), https://medium.com/coinbundle/utility-tokens-978d117290cd.
- Melanie Swan, 'Anticipating the economic benefits of blockchain' (October 2017), Technology Innovation Management Review, vol. 7, issue 10, p.6-14, available at https://timreview.ca/sites/default/files/Issue_PDF/TIMReview_October2017.pdf.
- Michael Pisa and Matt Juden, 'Blockchain and economic development: Hype vs. reality' (July 2017), CGD Policy Paper. Washington, DC: Center for Global Development, available at https://www.cgdev.org/publication/blockchain-and-economic-development-hype-vs-reality.
- Michèle Finck, 'Smart Contracts as a Form of Solely Automated Processing Under the GDPR' (January 8, 2019), Max Planck Institute for Innovation & Competition Research Paper No. 19-01., available at SSRN: https://ssrn.com/abstract=3311370 or http://dx.doi.org/10.2139/ssrn.3311370.
- Mike Orcutt, 'Once hailed as unhackable, blockchains are now getting hacked' (Feb 2019), MIT Technology Review, https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/.
- Nick Szabo, 'Smart Contracts: Building Blocks for Digital Markets' (1996), available at http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.
- Nick Szabo, 'Smart Contracts: Building Blocks for Digital Markets', EXTROPY: The Journal of Humanist Thought (1996), . available at http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.
- Niels Hackius and Moritz Petersen, 'Blockchain in logistics and supply chain: Trick or treat' (2017), Proceedings of the Hamburg International Conference of Logistics,

available at https://pdfs.semanticscholar.org/7752/f1275da69d208e5a76d7adc6b12b3b61699e.pdf.

- Niepmann Friederike and Tim Scmidt-Eisenlohr, 'International trade risk and the role of banks' (2015), International Finance Discussion Papers n° 1151, available at https://www.federalreserve.gov/econresdata/ifdp/2015/files/ifdp1151.pdf.
- Northeastern University, 'Guide to the rise of cryptocurrency (2019)', https://onlinebusiness.northeastern.edu/neu-msf/guide-to-the-rise-of-cryptocurrency-digital-currency-and-Bitcoin/.
- Norton Rose Fulbright, 'Unlocking the blockchain. A global legal and regulatory guide. Chapter 1: An introduction to blockchain technologies', https://www.nortonrosefulbright.com/en/knowledge/publications/0f7d02ac/unlocking-the-blockchain-a-global-legal-and-regulatory-guide---chapter-1.
- Olga Stashenko, 'Blockchain for know your customer (KYC): use cases' https://merehead.com/blog/blockchain-for-know-your-customer-kyc-use-cases.
- Open Access Government, '11 reasons for blockchain in public services' (2019), https://www.openaccessgovernment.org/blockchain-in-public-services/65941/.
- Paul Rosenzweig, 'Bad Code Is Already a Problem. Soon, Companies Will Be Liable' (July 2017), available at https://foreignpolicy.com/2017/07/28/bad-code-is-already-a-problem-soon-companies-will-be-liable/.
- Philipp Hacker and Chris Thomale, 'Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law' (Jan 2018), forthcoming in European Company and Financial Law Review, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820.
- Philipp Paech, 'Law and Autonomous System Series: What is a Smart Contract?' (July 2018) https://www.law.ox.ac.uk/business-law-blog/blog/2018/07/law-and-autonomous-systems-series-what-smart-contract.
- Philip Stafford, 'FT Explainer: The blockchain an financial markets' (2015), https://www.ft.com/content/454be1c8-2577-11e5-9c4e-a775d2b173ca.
- Polkadot, 'Walkthrough of Polkadot's Governance' (July 2019), https://polkadot.network/a-walkthrough-of-polkadots-governance/.
- Primavera De Filippi, Benedikt Schuppli, Cosntance Choi, Carla Reyes, Nikita Divissenko et al., 'Regulatory Framework for Token Sales: An Overview of Relevant Laws and Regulation in Different Jurisdictions'(Feb 2019), Research Report, Blockchain Research Institute and Coala, available at https://hal.archives-ouvertes.fr/hal-02046797/document.
- PwC, 'Global blockchain business survey: Blockchain is here what is your next move?' (2018), available at http://explore.pwc.com/blockchain/Exec-summary?WT.mc_id=CT11-PL1000-DM2-TR1-LS4-ND30-TTA5-CN_US-GX-xLoSBlockchain-LB-PwCExecSum&eq=CT11-PL1000-DM2-CN_US-GX-xLoSBlockchain-LB-PwCExecSum.
- PwC, 'How blockchain technology could impact HR and the world of work', available at https://www.pwc.co.uk/issues/futuretax/how-blockchain-can-impact-hr-and-the-world-of-work.html.
- Rakesh Sharma, 'Why a New 'Know you Customer' Project is Crucial to Blockchain' (June 2019), available at https://www.investopedia.com/news/why-new-know-your-customer-project-crucial-blockchain.
- Rebecca Campbell, 'Sweden Tests Blockchain Smart Contracts for Land Registry' (June 2016), https://cointelegraph.com/news/sweden-tests-blockchain-smart-contracts-for-land-registry.
- Reed, Chris and Sathyanarayan, Umamahesh and Ruan, Shuhui and Collins, 'Justine, Beyond Bitcoin – Legal Impurities and Off-Chain Assets' (October 2017), Queen Mary School of Law Legal Studies, Research Paper No. 260/2017, available at SSRN: https://ssrn.com/abstract=3058945 or http://dx.doi.org/10.2139/ssrn.3058945.

- Refinitiv, 'KYC Compliance: the rising challenge for corporates', available at https://www.refinitiv.com/content/dam/marketing/en_us/documents/reports/kyc-compliance-the-rising-challenge-for-corporates-special-report.pdf.
- Ren Zhang, Bart Preneel, 'Publish or Perish: A Backward-Compatible Defense against Selfish Mining in Bitcoin', KULeuven, available at https://www.esat.kuleuven.be/cosic/publications/article-2746.pdf.
- Report of the EU Blockchain Observatory and Forum, 'Legal and Regulatory Framework of Blockchains and Smart Contracts' (2019), available at https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf?width=1024&height=800&iframe=true.
- Reuters, 'U.S., EU fines on banks misconduct to top $400 billion by 2020-report' (Sept 2017), https://in.reuters.com/article/banks-regulator-fines/u-s-eu-fines-on-banks-misconduct-to-top-400-billion-by-2020-report-idINKCN1C210D.
- Richard Holden and Anup Malani, 'Can Blockchain Solve the Holdup Problem in Contracts?' (2017), available at https://www.law.northwestern.edu/research-faculty/colloquium/law-economics/documents/Malani_Blockchain.pdf.
- Richard Red, 'What is on-chain cryptocurrency governance? Is it plutocratic?' (June 2018), https://medium.com/@richardred/what-is-on-chain-cryptocurrency-governance-is-it-plutocratic-bfb407ef6f1.
- Robby Houben and Alexander Snyers, 'Cryptocurrencies and blockchain', Policy Department for Economic, Scientific and Quality of Life Policies, PE 619.024 (July 2018), http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf.
- Roman Beck, Christoph Müller-Bloch and John King, 'Governance in the Blockchain Economy: A Framework and Research Agenda' (2018), available at https://www.researchgate.net/publication/323689461.
- Roman Matzutt et al, 'A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin' (26 February 2018), available at https://fc18.ifca.ai/preproceedings/6.pdf.
- Ryan Browne, 'It costs $26,000 to mine one bitcoin in South Korea-and just $530 in Venezuela' (Feb 2018), https://www.cnbc.com/2018/02/15/the-cheapest-and-most-expensive-countries-to-mine-bitcoin.html.
- S. Howell, M. Niessner, D. Yermack, 'Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sale', European corporate governance institute, Finance Working Paper, n. 564/2018, available at https://ecgi.global/sites/default/files/working_papers/documents/finalhowellniessneryermack.pdf.
- Samburaj Das, 'Singapore Regulator, Bank Complete KYC Blockchain Prototype', https://www.ccn.com/singapore-regulator-banks-complete-kyc-blockchain-prototype/.
- Samuel Gibbs, 'Child abuse imagery found within Bitcoin's blockchain' (20 March 2018), https://www.theguardian.com/technology/2018/mar/20/child-abuse-imagery-bitcoin-blockchain-illegal-content.
- Santander Innoventures, 'The Fintech 2.0 Paper: Rebooting financial services' (2015), available at http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf
- Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2009), available at https://bitcoin.org/bitcoin.pdf.
- Sazandrishvili G., 'Asset tokenisation on blockchain explained in plain English' (2018), https://medium.com/coinmonks/asset-tokenization-on-blockchain-explained-in-plain-english-f4e4b5e26a6d.
- Scalability, interoperability and sustainability of blockchain, A Thematic Report prepared by the European Union Blockchain Observatory and Forum, available at

https://www.eublockchainforum.eu/sites/default/files/reports/report_scalaibility_06_03_2019.pdf?width=1024&height=800&iframe=true.

- Securities and Markets Stakeholders Group (SMSG) , 'Advice to ESMA: Own Initiative Report on Initial Coin Offerings and Crypto-Assets', available at: https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf.
- Shanhong Liu, 'Size of the Bitcoin blockchain from 2010 to 2019' (2019), https://www.statista.com/statistics/647523/worldwide-Bitcoin-blockchain-size/.
- Silke Elrifai et al., 'A Model Multilateral Treaty for the Encouragement of Investment in Climate Change Mitigation and Adaptation' (2019), Journal of International Arbitration, vol 36, n°1, available at http://www.kluwerlawonline.com/abstract.php?area=Journals&id=JOIA2019004.
- Sinclair Davidson, Primavera De Filippi, Primavera and Jason Potts, 'Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology' (July 19, 2016). Available at SSRN: https://ssrn.com/abstract=2811995 or http://dx.doi.org/10.2139/ssrn.2811995.
- Somto Kizor – Akaraiwe, 'Smart Contracts, Copyrights and Artificial Intelligence' (2019), available at https://www.researchgate.net/publication/335273097.
- Spyros Makridakis and Steven Wheelwright , 'Forecasting: Issues and challenges for marketing management' (1977), Journal of Marketing, available at https://www.researchgate.net/profile/Spyros_Makridakis/publication/270458049_Forecasting_Issues_Challenges_for_Marketing_Management/links/54be3bde0cf218d4a16a5590/Forecasting-Issues-Challenges-for-Marketing-Management.pdf.
- Stan Higgins, 'AXA Is Using Ethereum's Blockchain for a New Flight Insurance Product' (13 September 2017), https://www.coindesk.com/axa-using-ethereums-blockchain-new-flight-insurance-product.
- Stan Higgins, 'The EU is building a 'financial transparency gateway' (2017), https://www.coindesk.com/eu-developing-prototype-blockchain-platform-public-company-data.
- Statista, 'Global gross domestic product (GDP) at current prices from 2014 to 2024' (2019), https://www.statista.com/statistics/268750/global-gross-domestic-product-gdp/.
- Stephen O'Neal, 'Tokenisation explained' (2019), https://cointelegraph.com/explained/tokenization-explained.
- Steven Callander and Gregory Martin, 'Dynamic Policymaking with Decay. American Journal of Political Science' (2016), vol 61, issue 1, available at https://onlinelibrary.wiley.com/doi/abs/10.1111/ajps.12258.
- Suhyeon Lee, Seungjoo Kim, ' Pooled Mining Makes Selfish Mining Tricky'(22 Dec 2018), available at https://eprint.iacr.org/2018/1230.pdf.
- Teppo Felin and Karim Lakhani, 'What problems will you solve with blockchain' (September 2018), MIT Sloan Management Review, https://sloanreview.mit.edu/article/what-problems-will-you-solve-with-blockchain/.
- Thijs Maas, 'The Case for Hybrid Tokens' (26 June 2019), https://www.lawandblockchain.eu/the-case-for-hybrid-tokens/.
- Think BLOCK tank, 'The Regulations of Tokens in Europe, Parts A&B: The Eu legal and Regulatory Framework' (June 2019), available at https://distributed-ledger-consulting.de/wp-content/uploads/2019/08/thinkBLOCKtank-Token-Regulation-Paper-v1.0.pdf.
- Thomas Brewster, 'Why investors are betting millions on bitcoin surveillance' (April 2018), https://www.forbes.com/sites/thomasbrewster/2018/04/05/snooping-on-bitcoin-is-big-business/#77fccf002d19.
- Thorsten Koeppl and Jeremy Kronick, 'Blockchain technology: What is instore for Canada's economy and financial markets'(2017), CD Howe Institute Commentary

No. 468, available at https://www.cryptoninjas.net/wp-content/uploads/2017/09/Commentary_468_0.pdf.
- Tim Swanson, 'Who are the Administrators of Blockchains?' (October 2017), https://www.ofnumbers.com/2017/10/19/who-are-the-administrators-of-blockchains/.
- Tim Wu, 'Agency Threats' (2011), Duke Law Journal, vol 60:1841, available at https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1506&context=dlj.
- Tom Robinson, D.Phil & Yaya Fanusie, 'Bitcoin Laudering: An Analysis of Illicit Flows into Digital Currency Services' available at https://info.elliptic.co/whitepaper-fdd-bitcoin-laundering.
- UK CDC, 'Evaluating Policy Impact' (2017), available at https://www.cdc.gov/injury/pdfs/policy/Brief%205-a.pdf.
- UK Government Chief Scientific Adviser, 'Distributed Ledger Technology: Beyond Blockchain '(Jan 2016), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.
- United States volume of merchandise trade exports was US$ 1,482 billion in 2011 (United Nations Conference on Trade and Development, Statistics database 2018, https://unctad.org/en/PublicationsLibrary/ditctab2019d2_en.pdf.
- V. Buterin (October 2018) https://twitter.com/vitalikbuterin/status/1051160932699770882?lang=en.
- Visa Fact Sheet, https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf.
- West, 'The World Market for Cryptocurrency: 2017-2018 Review & 2019-2024 Forecast' (Sept 2019), https://www.globenewswire.com/news-release/2019/09/09/1912565/0/en/The-World-Market-for-Cryptocurrency-2017-2018-Review-2019-2024-Forecast-with-Analysis-on-Bitmain-Technologies-BitGo-NVIDIA-Corporation-Ripple-Networks-and-Coinbase.html.
- White and Case, 'International ICOs – legal challenges and implications' (2018), https://www.whitecase.com/publications/alert/international-icos-legal-challenges-and-implications.
- WHO, Growing threat from counterfeit medicines (2018), https://www.who.int/bulletin/volumes/88/4/10-020410/en/.
- Willem-Jan Smits, 'Blockchain governance: is it, what types are there and how does it work in practice', https://watsonlaw.nl/blockchain-governance-what-is-it-what-types-are-there-and-how-does-it-work-in-practice/.
- William Foxley, 'Exit Scams Swindled $3.1 Billion FromCrypto Inverstors in 2019: Report' (August 2019), https://www.coindesk.com/exit-scams-swindled-3-1-billion-from-crypto-investors-in-2019-report.
- William Foxley, 'Netherlands May Block Foreign Crypto Firms Under Anti-Money Laudering Laws' (Sept 2019), https://www.coindesk.com/dutch-interpretation-of-eu-anti-money-laundering-rules-may-block-foreign-firms.
- William Gordon and Christian Catalini, 'Blockchain technology for healthcare: Facilitating the transition to patient driven interoperability' (2018), available at https://www.sciencedirect.com/science/article/pii/S200103701830028X.
- The World Economic Forum, 'Building value with blockchain technology: How to evaluate blockchains benefits' (July 2019), available at http://www3.weforum.org/docs/WEF_Building_Value_with_Blockchain.pdf.
- World Economic Forum, 'The Future of Financial Services - How disruptive innovations are reshaping the way financial services are structured, provisioned and consumed' (June 2015), available at http://www3.weforum.org/docs/WEF_The_future__of_financial_services.pdf.
- World Payments Report 2018, https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/World-Payments-Report-WPR18-2018.pdf.

- World Economic Forum, 'Building blockchains for a better planet' (2018), http://www3.weforum.org/docs/WEF_Building-Blockchains.pdf.
- World Economic Forum, 'Building value with blockchain technology: How to evaluate blockchains benefits' (2019), available at http://www3.weforum.org/docs/WEF_Building_Value_with_Blockchain.pdf.
- WTO, International Trade Statistics (2015), available at https://www.wto.org/english/res_e/statis_e/its2015_e/its2015_e.pdf.
- Xiao Yue et al., 'Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control' (2016), available at https://link.springer.com/article/10.1007/s10916-016-0574-6.

Annex II – Interview reports (key stakeholders)

In this annex, please find the interview reports from the interviews with key stakeholders, as well as the template which was used to conduct these interviews.

Annex III – Legal research questionnaires

In this annex, please find the completed legal research questionnaires, as well as the legal research questionnaire template.

Annex IV – Interview reports (financial regulators)

In this annex, please find the interview reports from the interviews with key stakeholders, as well as the template which was used to conduct these interviews.

Annex V – Briefing document and questionnaire

This annex contains the briefing document and questionnaire used in the first round of Delphi consultation. The document was emailed to approximately 200 blockchain experts, including industry representatives, entrepreneurs, policy makers, economists, lawyers and other stakeholder groups. A slightly amended version of the questionnaire was distributed to participants at the blockchain workshop held in Brussels on 2 December 2019.

European Commission

Study on Blockchains: Legal, governance and interoperability aspects (SMART 2018/0038)

Luxembourg, Publications Office of the European Union

2020

ISBN 978-92-76-16306-0
doi: 10.2759/4240

KK-03-20-092-EN-N

doi: 10.2759/4240 ISBN 978-92-76-16306-0

Publications Office
of the European Union