European Commission

Framework Contract JUST/2020/PR/03/0001

Study on civil law rules applicable to smart contracts JUST/2021/PR/SMART/CIVI/0111

Final report

Written by: VVA, London Economics, Datarella,
Prof. Michèle Finck, CSES
November 2023

EUROPEAN COMMISSION

Directorate-General for Justice and Consumers
Directorate A — Justice Policies
Unit A.1 — Digital Transition and Judicial Training

Contact: JUST-A1@ec.europa.eu

European Commission
B-1049 Brussels

EUROPEAN COMMISSION

Framework Contract JUST/2020/PR/03/0001

Study on civil law rules applicable to smart contracts JUST/2021/PR/SMART/CIVI/0111 Final report

Final report

Directorate-General for Justice and Consumers
Novel Forms of Contracting in the Digital Economy

2023

EUR EN

Manuscript completed in November 2023

This document has been prepared for the European Commission however it reflects the views only of the authors, and the European Commission is not liable for any consequence stemming from the reuse of this publication.

European Union, 2023

Table of Contents

List of Tables

List of Figures

Abstract

This report is the result of the study on civil law rules applicable to smart contracts, under DG JUST's Framework Contract JUST/2020/PR/03/0001 for Evaluation, Impact Assessment and Related Policy Support Services in the Justice and Consumers Policy Areas carried out by VVA, Datarella, London Economics, Prof. Michèle Finck and CSES.

The main objectives of this report are twofold: (i) allow the Commission to assess the existence and effect of civil law obstacles to the deployment and use of smart contracts in the EU single market, and (ii) provide insights on the potential and feasibility of personal data management tools based on smart contracts.

For that purpose, the report provides: (i) an analysis of the economic features of smart contracts, (ii) a comparative analysis of civil law rules in the 30 Member States of the European Economic Area, (iii) a technical feasibility assessment and a feasibility matrix which creates a path for understanding the feasibility of applying technical solutions to identified legal challenges, and (iv) a comprehensive analysis of the potential of distributed ledger technologies and smart legal contracts regarding access to and sharing of personal data, specifically in respect of personal data management tools.

Sommaire

Ce rapport est le résultat de l'étude sur les règles de droit civil applicables aux contrats intelligents, au titre du contrat-cadre JUST/2020/PR/03/0001 de la DG JUST pour l'évaluation, l'analyse d'impact et les services de soutien politique connexes dans les domaines politiques de la justice et des consommateurs, réalisée par VVA, Datarella, London Economics, la professeur Michèle Finck, et CSES.

Les principaux objectifs de ce rapport sont doubles : (i) permettre à la Commission d'évaluer l'existence et l'effet des obstacles de droit civil au déploiement et à l'utilisation des contrats intelligents dans le marché unique de l'UE, et (ii) donner un aperçu du potentiel et de la faisabilité des outils de gestion des données personnelles basés sur les contrats intelligents.

À cette fin, le rapport fournit : (i) une analyse des caractéristiques économiques des contrats intelligents (ii) une analyse comparative des règles de droit civil dans les 30 États membres de l'Espace économique européen (iii) une évaluation de la faisabilité technique et une matrice de faisabilité qui crée une voie pour comprendre la faisabilité de l'application de solutions techniques aux défis juridiques identifiés, et (iv) une analyse complète du potentiel des technologies de registres distribués et des contrats juridiques intelligents en ce qui concerne l'accès aux données personnelles et leur partage, en particulier concernant les outils de gestion des données personnelles.

Executive summary

This document constitutes the Final Report of the study on civil law rules applicable to smart contracts, under DG JUST's Framework Contract JUST/2020/PR/03/0001 for Evaluation, Impact Assessment and Related Policy Support Services in the Justice and Consumers Policy Areas.

The overall objective of the study was to assess the legal and technical feasibility of implementing smart contracts within the European Economic Area (EEA), both in Business to Business (B2B) and Business to Consumer (B2C) relations. The concrete aims of the study were to:

- identify existing obstacles caused by national-level measures for the use of smart contracts based on distributed ledger technology (DLT), including the extent and the economic context of these problems; and
- provide an overview of possible technical solutions applied to smart contracts, and an assessment of the overall potential of DLT and smart legal contracts in terms of data sharing, particularly by personal data management tools.

To meet these objectives, data was collected *inter alia* through national legal research, interviews, literature reviews and the examination of specific use cases.

At the time of writing, three EEA Member States have legislation on smart contracts, while the remaining EEA Member States do not have such provisions. It should be noted that some EEA Member States have made steps towards the possible future regulation of smart contracts, either by developing a draft law or creating legislation on distributed ledger technology (DLT). Since only a handful of EEA Member States have rules specifically applicable to smart contracts and/or DLT, smart contracts in other EEA Member States remain covered – in several cases – by the national general legal regime applicable to contracts. As the findings of this study show, this situation foreshadows several challenges for the use of smart contracts across a wide variety of sectors that could eventually – in the absence of suitable regulation – create potential obstacles within the internal market. However, existing legal or technical obstacles could not be proven within the internal market, due to the very limited use of smart contracts and the limited available evidence base at this stage, but legal challenges linked to their use are identified below.

The study examined several aspects of contract law in relation to smart contracts. Particularly, it explored national rules on contract formation, rules setting out form requirements, contract interpretation and evidential value, as well as the rules on the termination of contracts and remedies.

Regarding contract formation, the main principle applicable to contracts in all EEA Member States is the principle of freedom of form, which allows parties to decide the form of the contract. Generally, the contract is considered to have been formed when the offeror receives the acceptance of the offer. This acceptance can be done tacitly or through performance in some EEA Member States. The principle of freedom of form prevails unless

the law contains specific form requirements. While the eIDAS Regulation[1] covers a rather wide range of contracts and allows them to be considered as meeting the form requirements when signed with an authenticated electronic signature, rules on specific forms (such as notarial authentication or registration with public authorities) can represent a challenge from a legal perspective if requirements of such formalities cannot be met by the smart contracts technology. Notably, in some cases, certain types of contracts are more heavily regulated and have stringent form requirements (e.g., property law). However, as the technical analysis and the case studies indicate, compliance with such rules on specific forms can be possible.

Additional challenges can be found in relation to B2C contracts, which entail more requirements for businesses to protect the consumer. This includes, for instance, the consumer's right of withdrawal within 14 days of signing the contract or information requirements. More specifically, the right of withdrawal can be difficult to ensure because of the immutability of blockchain, while meeting information requirements can be challenging, since the language of the code may not be deemed as clear, specific, and legible for consumers. The identification of the parties was also found to be a challenge for smart contracts, as in some cases (for example, in the case of public permissionless blockchains) it can remain uncertain who exactly is behind the screen as a party to the contract. In this light, the issue of legal capacity of parties arises, since it may be difficult to determine whether the party has the legal capacity required for the specific type of contract into which he/she is entering. It should be noted that the issue of legal capacity, while particularly crucial for B2C contracts, is also relevant for B2B contracts.

Rules on interpretation of contracts and their evidential value show similarities in EEA Member States, and consequently the challenges indicated also show a similar pattern. A major challenge in this regard could stem from the immutable nature of smart legal contracts. In such cases, it would be difficult to explore the intention of contracting parties through a programme code on which a smart legal contract is based (especially when interpreting more abstract clauses of contract law), although, this can be alleviated by providing a natural language version of the contract in parallel. Furthermore, another significant challenge for smart contracts is rooted in divergent contract law rules regarding documents bearing full evidential value. However, two EEA Member States (Greece and Italy), with specific legislation on smart contracts, vest smart contracts with full evidential value, indicating that potential future obstacles could be overcome in this regard.

In terms of contract termination rules and remedies, contract laws of EEA Member States are similar. Prime potential challenges in this area are based on the immutable nature of smart contracts, as well as the limits of adding specific elements (such as "good faith", "best efforts", "reasonable period" etc) whose objective assessment is difficult. Furthermore, it is difficult to interpret the provisions of a smart contract without the appropriate technical expertise. This can lead to complications when it comes to understanding code language, given that, an incorrect interpretation of contractual clauses could lead to errors in fulfilling obligations or exercising rights.

There is – at the time of writing – no empirical evidence that would suggest that the existing general national civil law rules (which, as explained above, are similar across the EEA

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation).

Member States) constitute obstacles for stakeholders using smart contracts within the internal market. This may, however, be due to the currently still very limited uptake of smart contracts (see further below) rather than the law itself. Thus, while current similar rules do not constitute an obstacle, the introduction of divergent rules can increase the possibility of the current challenges turning into obstacles.

When considering how smart contracts operate in practice, there are different viewpoints to consider. From a legal/regulatory perspective, these can include differences in legal regimes, recognition of smart contracts and how they are defined both at the policy level and at law. Then there are the different ways smart contracts are deployed based on the needs of the blockchain, its underlying consensus mechanism, and how smart contracts get integrated into different, complex business cases. Different financial products, such as automated market makers are also enabled thanks to smart contracts. Smart contracts help support new types of financial services such as pay-per-use models and fractionalisation. Smart contracts are used to support track-and-trace business case for supply chain logistics and can be leveraged for digital identity schemas. Smart contracts are also increasingly being integrated into IoT use cases involving mobility and smart devices.

Moreover, smart contracts overarchingly help facilitate services that are cross border. The jurisdiction(s) where the smart contracts will be deployed plays a role in how consumer protection, data protection, operational security and other regulations affect the smart contract. This in turn plays a role in how, from a technical perspective, the smart contract performs its designated functions at the use-case level.

While the study found no evidence that smart contracts using DLT are currently generating economic value for users in the EU[2], potential use cases for DLT-based smart contracts exist in important sectors of the economy (financial services, data management, communication) and in important emergent technologies (autonomous systems, PIMS). Cross-border transactions may be assumed to provide some particularly attractive use cases because the lower per-execution cost of smart contracts is especially cost-effective.

This study relied on comparative law analysis to determine the most commonly recurring challenges to the use of smart contracts in the EU/EEA. In line with the above, several recurring challenges were identified, such as: counterparty identification and agreement, requirements for B2C contracts,[3] specific contract forms, the immutability of blockchains etc.

In view of these challenges, it can be argued that B2B markets, where there are fewer constraints on contract formation, are more likely to see widespread uptake of smart contract solutions in the near term.

[2] The cost of current DLT-enabled smart contract solutions is high, and economic operation depends on a minimum efficient scale that is currently not achieved at the market level (profitable examples may exist at the enterprise level and in one-off projects).

[3] While this was identified as a challenge from a civil law perspective, it is negligible from a techno-economic perspective. In other words, the B2C requirements are a challenge in legal terms rather than a market mechanism issue.

The study examined the technical feasibility of solutions that also include those identified under the draft Data Act[4] to discover whether there are technical means to overcome the identified challenges. The technical solutions examined were both specific and broadly related to enabling supervision over smart contract regimes in compliance with existing civil law provisions and EU regulations:

- Programming languages and available methods.
- Compliance with existing consumer protection at the code level.
- Reverse transaction features.
- Safe termination in smart contract design.
- Dispute resolution in smart contract design.
- Counterparty identification and smart contract-based liability assignment.
- 'Embedded supervision' in 'permissioned' DLT environments leveraging on-chain data.

To bridge the challenges and technical feasibility solutions, a case study analysis was undertaken using qualitative interviews with companies currently working on different smart contract solutions or otherwise already deploying them actively. The case studies were based on interviews with deltaDAO AG, CashOnLedger and Bosch GmbH. The three companies vary greatly in both the percentage of DLT technology used and smart contract design. The DLT component ranges from less than 10% of the total business model in the case of CashOnLedger to almost 100% in the case of deltaDAO. In all three cases, the execution of contractual obligations can occur both on and off-chain. On-chain supervision was identified as a powerful tool to monitor the activity and safety of blockchain networks. Any steps to create an embedded supervisory regime for smart contracts would have to carefully balance reducing the cost of compliance and enforcing a level playing field.

Where the draft Data Act requires terminability for smart contracts there is a need to clarify that implementing such requirements on permissionless public blockchains could create additional compliance challenges to those networks due to their degree of openness. This includes allowing anyone to read, write and participate in validating network consensus on a public permissionless protocol. Although the draft Data Act does not explicitly provide for the inclusion of reverse transaction features, these features are a technical abstraction connected to the immutability of smart contracts (which was identified as a challenge in the comparative law analysis). Therefore, these features are an important unit of analysis for the study. The study findings suggest that reverse transactions could lead to new forms of ledger-based chargeback fraud in reversible smart contracts.

Digital identity schemas were identified as a crucial sub-category that could solve both counter-party identification obstacles and address data protection concerns. However, without clearer policy guidance on evolving concepts of identity, also for the machine economy, Europe risks losing a competitive advantage in Industry 4.0. Guidance on digital identity would also clarify some of the challenges European start-ups currently face in designing use-cases for cross-sectoral data exchange where that data is transmitted

[4] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN. It should be noted that this study examined the abovementioned draft Data Act, while it touched upon the European Parliament's amendments to the draft Data Act adopted on 14 March 2023 only where particularly important as its publication overlapped with the delivery of this final report.

between machines and not only natural or legal persons. Novel identity primitives such as SoulBound Tokens were examined as a way to embed compliance and overcome information asymmetries in decentralised market processes borne from pseudonymity (e.g., in decentralised finance).

Finally, it would be important to view smart contracts as constantly evolving. Smart contracts exist on a spectrum between 100% interoperability on the one hand and 100% legal certainty[5] on the other. Challenges and technical solutions identified in this report act upon smart contracts as they oscillate between interoperability and legal certainty. Examples include the IP challenges of transferring in-game items represented as NFTs or the employment of smart contracts within decentralised autonomous organisations and their broader legal (un)certainty. Today, there is no legal or technical solution that can achieve a total equilibrium between these two poles; this is an important consideration for policy makers.

The study also examined the potential of smart legal contracts, namely legally binding contracts in which, either some or all of the associated terms, conditions and rights under the contract are defined in and/or performed by code execution, in the context of enabling access to and sharing of personal data, specifically in respect of personal data management tools. This analysis was undertaken against the background of the draft Data Act, which would, inter alia, introduce a new data access regime for IoT data. Given that the Data Act had not yet been finalised at the time of conducting our research, our findings are based on the Commission proposal.

DLT combined with smart legal contracts enable the distributed recording of encrypted data. This can generate efficiency gains and create incentive mechanisms that can result in new markets for data. Some industry experts and literature predict that personal data management tools using blockchain-based smart contracts will be vital components to realise the data-sharing objectives under the draft Data Act, namely the Commission's proposal.

From the outset, it must be noted that Personal Information Management Systems (PIMS) are a broad category of techno-organisational tools that leverage different combinations of technical elements, sometimes also smart legal contracts, with the shared objective of giving their users more transparency and control over their personal data.

There can be no doubt that new technical interfaces are needed to realise the portability right foreseen in Articles 3-7 of the draft Data Act. This regime requires that individuals exercise personal initiative to invoke this new right to informational self-determination. Yet, experience in EU data law so far, such as regarding the right to the portability of personal data under Article 20 GDPR, has shown that individuals only rarely take such initiative in relation to their data. Technical tools such as PIMS could render related processes more efficient and transparent, thereby lowering existing barriers to personal initiative. Whereas this is considered to directly benefit data users, including data subjects, and gives them

[5] Legal certainty is here meant to reference the evolving legal standing of smart contracts at European law. Examples included but are not limited to whether smart contracts are permissible in court proceedings, can provide adequate levels of consumer protection, and data protection. It also refers to whether the technical abstractions that smart contracts make possible are further compatible with B2B contracts referencing the transfer of title, and ownership of property which increasingly includes 'real world' tokenized assets. Interoperability refers to the complex and evolving nature of network compatibility between different sovereign blockchains and the challenges of reconciling cross-chain activity.

more transparency and practical control over the processing of personal data that relates to them, this would also help to achieve the draft Data Act's underlying objectives of increasing access to and sharing of data. In turn, this could drive data-related innovations and increase the competitiveness of the internal market.

At the time of writing, PIMS are still a nascent category with varying structures, business models and technical backbones. This study provides an overview of the various features of PIMS such as their business models, data storage, technical design and services offered, before highlighting the challenges and limitations they still face.

The study confirms that PIMS using smart legal contracts can facilitate the conclusion of a contract between the data holder and the data user and that they can be helpful tools to enable access to data after a simple request through electronic means. We also find that PIMS can also help enable data users to easily verify their own identity and facilitate data holders' management of user information. Beyond, PIMS can also help enable data holders to determine whether there is a valid legal basis, such as consent or contract, to access personal data or to determine document the purpose of personal data processing and to help ensure compliance with the GDPR's regime on data subject rights and the transparency principle under the GDPR.

Smart legal contracts are particularly helpful under Articles 3-5 of the draft Data Act, which foresees contractual relations between all parties, as they can automate the conclusion and execution of such contracts subject to the limitations identified through the comparative civil law analysis in this study and hence reduce the costs associated with data sharing.

PIMS using smart legal contracts must be careful to abide by the various legal requirements under the draft Data Act and they must furthermore be designed to account for different interests, such as those of the consumer and the trader respectively, where consumer protection law is applicable, as well as the respective interests of the data subject and the data controller.

The study provides two tools that could remedy some of these concerns: interoperability (subject to some caveats), as well as model contractual terms. These two tools could, on the one hand, encourage the proliferation of suitable PIMS using smart legal contracts in the Digital Single Market and, on the other, make it more attractive for relevant actors to rely on PIMS using smart contracts.

Résumé

Ce document constitue le rapport final de l'étude sur les règles de droit civil applicables aux contrats intelligents, au titre du contrat-cadre JUST/2020/PR/03/0001 de la DG JUST pour l'évaluation, l'analyse d'impact et les services d'appui stratégique connexes dans les domaines politiques de la justice et des consommateurs.

L'objectif global de l'étude était d'évaluer la faisabilité juridique et technique de la mise en œuvre des contrats intelligents dans l'Espace économique européen (EEE), à la fois dans les relations entre entreprises (B2B) et entre entreprises et consommateurs (B2C). Les objectifs concrets de l'étude étaient les suivants :

- Identifier les obstacles existants causés par les mesures prises au niveau national pour l'utilisation des contrats intelligents basés sur la technologie des registres distribués (DLT), y compris l'étendue et le contexte économique de ces problèmes ; et
- Fournir une vue d'ensemble des solutions techniques possibles appliquées aux contrats intelligents et une évaluation du potentiel global de la DLT et des contrats juridiques intelligents en termes de partage des données, en particulier par le biais d'outils de gestion des données personnelles.

Pour atteindre ces objectifs, des données ont été recueillies, entre autres, par le biais de recherches juridiques nationales, d'entretiens, d’analyse documentaire et de l'examen de cas d'utilisation spécifiques.

Au moment de la rédaction du présent rapport, trois États membres de l’EEE disposent d'une législation sur les contrats intelligents, tandis que les autres États membres de l’EEE ne disposent pas de telles règles. Il convient de noter que certains États membres de l’EEE ont pris des mesures en vue d'une éventuelle réglementation future des contrats intelligents, soit en élaborant un projet de loi, soit en adoptant une législation sur la technologie des registres distribués (DLT). Étant donné que seule une poignée d'États membres de l’EEE disposent de règles spécifiquement applicables aux contrats intelligents et/ou à la DLT, les contrats intelligents dans les autres États membres de l’EEE restent couverts, dans plusieurs cas, par le régime juridique national général applicable aux contrats. Comme le montrent les résultats de cette étude, cette situation laisse présager plusieurs défis pour l'utilisation des contrats intelligents dans un large éventail de secteurs qui pourraient éventuellement - en l'absence d'une réglementation appropriée - créer des obstacles potentiels au sein du marché intérieur. Cependant, aucun obstacle juridique ou technique n’a été prouvé au sein du marché intérieur, en raison de l’utilisation très limitée des contrats intelligents et du caractère limité des sources de données à l’heure actuelle mais les difficultés juridiques liées à leur utilisation sont identifiées ci-après.

L'étude a examiné plusieurs aspects du droit des contrats en relation avec les contrats intelligents. En particulier, elle a exploré les règles nationales en matière de formation des contrats, d’exigences de forme, d'interprétation des contrats et de leur valeur probante, ainsi que de résiliation des contrats et de recours contractuels.

Concernant la formation des contrats, le principe fondamental applicable aux contrats dans tous les États membres de l’EEE est le principe de la liberté de forme, qui permet aux parties de décider de la forme du contrat. De manière générale, le contrat est considéré comme formé lorsque l'offrant reçoit l'acceptation de l'offre. Cette acceptation peut se faire

tacitement ou par exécution du contrat dans certains États membres de l'EEE. Le principe de la liberté de forme prévaut, à moins que la loi ne contienne des exigences de forme spécifiques. Bien que le règlement eIDAS couvre un éventail assez large de contrats et permette de les considérer comme satisfaisants aux exigences de forme lorsqu'ils sont signés avec une signature électronique authentifiée, des règles spécifiques de forme (telles que l'authentification notariale ou l'enregistrement auprès des autorités publiques) peuvent représenter un défi d'un point de vue juridique, si ces exigences de forme ne peuvent pas être satisfaites par la technologie applicable aux contrats intelligents. En particulier, certains types de contrats sont fortement réglementés et présenteront des exigences strictes en matière de forme (par exemple, s'agissant du droit des biens). Néanmoins tel qu'indiqué par l'analyse technique et les études de cas, le respect de ces règles spécifiques de forme demeure possible.

Des défis supplémentaires peuvent exister s'agissant des contrats B2C, qui impliquent davantage d'exigences pour les entreprises afin de protéger le consommateur. Il s'agit, par exemple, du droit de rétractation du consommateur dans les 14 jours suivant la signature du contrat ou des exigences en matière d'information. Plus précisément, le droit de rétractation peut être particulièrement difficile à garantir en raison de l'immuabilité de la technologie de la chaîne de blocs (ou « blockchain »), tandis que garantir des exigences en matière d'information peut également s'avérer difficile, car le langage du code peut ne pas être considéré comme clair, spécifique et lisible pour les consommateurs. L'identification des parties peut aussi représenter un défi pour les contrats intelligents, car dans certains cas (par exemple, dans le cas des chaînes de blocs ou « blockchains » publiques sans permission), il peut être difficile de savoir qui est exactement derrière l'écran en tant que partie au contrat. Dans ce contexte, la question de la capacité juridique des parties se pose, car il peut être difficile de déterminer si la partie a la capacité juridique requise pour le type spécifique de contrat qu'elle conclut. Il convient de noter que la question de la capacité juridique, bien que particulièrement cruciale pour les contrats B2C, est également pertinente pour les contrats B2B.

Les règles relatives à l'interprétation des contrats et à leur valeur probante présentent des similitudes entre les États membres, conduisant ainsi à des défis au schéma similaire. À cet égard, un enjeu majeur pourrait résulter de la nature immuable des contrats juridiques intelligents. Dans de tels cas, il serait difficile d'explorer l'intention des parties contractantes à travers un code de programme sur lequel un contrat juridique intelligent est basé (en particulier l'interprétation de clauses plus abstraites du droit des contrats), bien que cela puisse être atténué en fournissant une version en langage naturel du contrat. En outre, un autre défi important pour les contrats intelligents provient des règles divergentes du droit des contrats en ce qui concerne les documents ayant une pleine valeur probante. Néanmoins, deux États membres (la Grèce et l'Italie) disposent d'une législation spécifique sur les contrats intelligents leur conférant ainsi une valeur probante totale, ce qui indique que des obstacles potentiels pourraient être surmontés à l'avenir à cet égard.

Le droit des contrats des États membres de l'EEE est similaire en ce qui concerne les dispositions relatives à la résiliation des contrats et les voies de recours contractuels. Les principaux défis potentiels dans ce domaine reposent sur la nature immuable des contrats intelligents, ainsi que sur les limites de l'ajout d'éléments spécifiques (tels que la 'bonne foi', 'obligation de moyens', et 'délais raisonnables' dont l'évaluation objective est difficile. En outre, il est difficile d'interpréter les dispositions d'un contrat intelligent sans expertise technique adéquate. Ceci peut mener à des complications s'agissant de la compréhension du langage codé ; d’autant plus qu’une mauvaise interprétation des clauses du contrat peut générer des erreurs dans l’exercice des droits ou l’exécution d’obligations.

Au moment de la rédaction de la présente étude, aucune preuve empirique ne suggère que les règles générales nationales du droit civil (qui, tel que développé ci-dessus, sont similaires d’un État membre de l’EEE à l’autre) constituent des obstacles pour les acteurs faisant usage des contrats intelligents au sein du marché intérieur. Cela pourrait néanmoins être due à l’usage actuellement peu fréquent des contrats intelligents (voir ci-dessous) plutôt qu’au droit lui-même. Donc, bien que les règles actuelles similaires ne constituent pas un obstacle, l’introduction de règles divergentes peut accroitre la possibilité que les défis actuels deviennent des obstacles.

L’examen de l’application pratique des contrats intelligents doit prendre en compte différents points de vue. D'un point de vue juridique et réglementaire, il peut s'agir de différences dans les régimes juridiques, de la reconnaissance des contrats intelligents et de la manière dont ils sont définis au niveau politique et juridique. Il y a également les différentes manières dont les contrats intelligents sont déployés en fonction des besoins de la blockchain, de leur mécanisme de consensus sous-jacent et de la façon dont les contrats intelligents sont intégrés dans différents cas d'affaires complexes. Différents produits financiers, tels que les teneurs de marché automatisés, sont également possibles grâce aux contrats intelligents. Les contrats intelligents aident à soutenir de nouveaux types de services financiers tels que les modèles de paiement à l’utilisation et le fractionnement. Les contrats intelligents sont utilisés pour soutenir l’analyse de rentabilisation de suivi et de traçabilité pour la logistique de la chaine d’approvisionnement et peuvent être exploités pour les schémas d’identité numérique. Les contrats intelligents sont également de plus en plus intégrés dans les cas d’utilisation de l’IdO impliquant la mobilité et les appareils intelligents.

De plus, les contrats intelligents contribuent de manière générale à faciliter les services transfrontaliers. La juridiction dans laquelle le contrat intelligent sera déployé joue un rôle dans la manière dont la protection des consommateurs, la protection des données, la sécurité opérationnelle et d'autres réglementations affectent le contrat intelligent. Cela joue également un rôle dans la manière dont, d'un point de vue technique, le contrat intelligent remplit les fonctions qui lui sont assignées au niveau du cas d'utilisation.

Bien que l'étude n'ait pas démontré que les contrats intelligents utilisant la DLT génèrent actuellement une valeur économique pour les utilisateurs dans l'UE[6], des cas d'utilisation potentiels pour les contrats intelligents basés sur la DLT existent dans des secteurs importants de l'économie (services financiers, gestion des données, communication) et dans des technologies émergentes importantes (systèmes autonomes, PIMS).[7] On peut supposer que les transactions transfrontalières offrent des cas d'utilisation particulièrement

[6] Le coût des solutions actuelles de contrats intelligents basés sur la DLT est élevé et leur exploitation économique dépend d'une échelle minimale efficace qui n'est actuellement pas atteinte au niveau du marché (des exemples rentables peuvent exister au niveau de l'entreprise et dans des projets ponctuels).

[7] Les avantages économiques des contrats intelligents basés sur la blockchain sont plus susceptibles d'être présents sur les marchés à fort volume (en termes d'un grand nombre de participants au marché, d'un grand nombre de transactions, ou les deux). Les services financiers, la gestion des données et l'itinérance en gros en sont des exemples.
Les applications B2B sont plus susceptibles d'être adoptées car elles sont soumises à moins de contraintes en matière de conclusion de contrats. En outre, le déploiement est plus facile sur les marchés où la complexité des transactions est faible et où les transactions restent dans la chaîne, sans qu'il soit nécessaire de les convertir fréquemment dans une autre monnaie.

attrayants, car le coût d'exécution plus faible des contrats intelligents est particulièrement rentable.

Cette étude s'est appuyée sur une analyse de droit comparé pour déterminer quels étaient les défis les plus récurrents concernant l'utilisation des contrats intelligents dans l'UE/EEE. Comme indiqué ci-dessus, plusieurs défis récurrents ont été identifiés, tels que l 'identification et l'accord des cocontractants, les exigences relatives aux contrats d'entreprise à consommateur (B2C)[8], les formes de contrats spécifiques et ; l'immuabilité des chaînes de blocs ou « blockchains » etc. Compte tenu de ces défis, il apparaît plus probable que des solutions de contrats intelligents pour les marchés B2B, lesquels présentent moins de contraintes en matière de formation des contrats, soient adoptées à grande échelle à court terme.

L'étude a examiné les solutions de faisabilité technique qui comprennent également celles identifiées dans le cadre de la proposition de règlement « Loi sur les données » afin d'identifier s'il existe des moyens techniques pour surmonter les défis identifiés. Les solutions techniques sont à la fois spécifiques et largement liées à la possibilité de superviser les régimes de contrats intelligents en conformité avec les dispositions de droit civil existantes et les règlements de l'UE :

- Langages de programmation et méthodes disponibles.
- Conformité avec la protection des consommateurs existante au niveau du code.
- Fonctionnalités d'inversion de transaction.
- Résiliation sécurisée dans la conception des contrats intelligents.
- Résolution des litiges dans la conception des contrats intelligents.
- Identification du cocontractant et attribution de la responsabilité sur la base d'un contrat intelligent.
- Supervision intégrée dans les environnements DLT "autorisés" exploitant les données de la chaîne.

Pour faire le lien entre les défis et les solutions de faisabilité technique, une analyse d'études de cas a été entreprise à l'aide d'entretiens qualitatifs auprès d'entreprises travaillant actuellement sur différentes solutions de contrats intelligents ou les déployant déjà activement. Les études de cas étaient basées sur des entretiens avec deltaDAO AG, CashOnLedger et Bosch GmbH. Les trois entreprises varient considérablement en ce qui concerne le pourcentage de technologie DLT utilisée et la conception des contrats intelligents. La composante DLT va de moins de 10 % du modèle commercial total dans le cas de CashOnLedger à près de 100 % dans le cas de deltaDAO AG. Dans les trois cas, l'exécution des obligations contractuelles a lieu à la fois en ligne et hors ligne. La supervision en chaîne a été identifiée comme un outil puissant pour contrôler l'activité et la sécurité des réseaux de blockchain. Toute mesure visant à créer un régime de surveillance intégré pour les contrats intelligents devra être soigneusement équilibrée entre la réduction du coût de mise en conformité et l'application de règles du jeu équitables.

Alors que la proposition de règlement « Loi sur les données » exige que les contrats intelligents soient résiliables, il est important de souligner que de telles exigences relatives

[8] Bien que cela ait été identifié comme un défi du point de vue du droit civil, il est négligeable du point de vue technico-économique. En d'autres termes, les exigences relatives aux contrats d'entreprise a consommateur (B2C) constituent un défi en termes juridiques plutôt qu'une question de mécanisme de marché.

aux blockchains publiques sans autorisation pourrait créer des défis de mise en conformité supplémentaires pour ces réseaux en raison de leur degré d'ouverture. Il s'agit notamment de permettre à quiconque de lire, d'écrire et de participer à la validation du consensus du réseau sur la base d'un protocole public sans autorisation. Bien que la proposition de règlement « Loi sur les données » n'exige pas explicitement l'inclusion de fonctionnalités de transactions inversées, ces fonctionnalités sont une abstraction technique connectée à l'immutabilité des contrats intelligents (qui a été identifiée comme un défi dans l'analyse de droit comparé), ce qui en fait un point d'analyse important pour l'étude. Les résultats suggèrent que les transactions inversées pourraient conduire à de nouvelles formes de fraude par rétro facturation dans les contrats intelligents réversibles.

Les schémas d'identité numérique ont été identifiés comme une sous-catégorie cruciale qui pourrait résoudre à la fois les obstacles à l'identification du cocontractant et répondre aux préoccupations en matière de protection des données. Toutefois, en l'absence d'orientations politiques plus claires sur les concepts évolutifs d'identité, y compris pour l'économie des machines, l'Europe risque de perdre un avantage concurrentiel dans l'industrie 4.0. Des orientations sur l'identité numérique permettraient également de clarifier certains des défis auxquels les start-ups européennes sont actuellement confrontées dans la conception de cas d'utilisation pour l'échange de données intersectorielles lorsque ces données sont transmises entre machines et pas seulement entre des personnes physiques ou morales. De nouvelles données d'identité telles que « SoulBound Tokens » ont été considérées comme un moyen d'intégrer la conformité et de surmonter les asymétries d'information dans les processus de marché décentralisés découlant du pseudonymat (par exemple dans le domaine de la finance décentralisée).

Enfin, il est important de considérer les contrats intelligents comme étant en constante évolution. Les contrats intelligents existent sur un gradient entre une interopérabilité à 100 % d'une part et une certitude juridique à 100 % d'autre part. Les défis et les solutions techniques identifiés dans ce rapport agissent sur les contrats intelligents lorsqu'ils oscillent entre l'interopérabilité et la sécurité juridique. On peut citer comme exemples les défis concernant la propriété intellectuelle liés au transfert d'objets présents dans des jeux et représentés par des NFT ou l'utilisation de contrats intelligents au sein d'organisations autonomes décentralisées et leur (in)certitude juridique plus large. Aujourd'hui, il n'existe pas de solution juridique ou technique permettant d'atteindre un équilibre total entre ces deux pôles, ce qui constitue une considération importante pour les décideurs politiques.

L'étude examine également le potentiel des contrats juridiques intelligents, à savoir des contrats juridiquement contraignants dans lesquels tout ou partie des termes, conditions et droits associés au contrat sont définis et/ou exécutés par code, dans le contexte de l'accès et du partage des données à caractère personnel, en particulier en ce qui concerne les outils de gestion des données à caractère personnel. Cette analyse s'inscrit dans le contexte de la proposition de règlement « Loi sur les données », qui introduirait, entre autres, un nouveau régime d'accès aux données pour les données de l'IdO. Étant donné que, au moment où nous avons mené nos recherches, la loi sur les données n'avait pas encore été finalisée, nos conclusions sont basées sur la proposition de la Commission.

Les technologies DLT combinées à des contrats juridiques intelligents permettent l'enregistrement distribué de données cryptées. Cela peut générer des gains d'efficacité et créer des mécanismes d'incitation qui peuvent aboutir à de nouveaux marchés pour les données. Certains experts du secteur et données de littérature prédisent que les outils de gestion des données personnelles utilisant des contrats intelligents basés sur la blockchain seront des éléments essentiels pour réaliser les objectifs de partage des données dans le cadre de la proposition de règlement « Loi sur les données », c'est-à-dire la proposition de la Commission.

D'emblée, il convient de noter que les systèmes de gestion des informations personnelles (PIMS) constituent une vaste catégorie d'outils technico-organisationnels qui tirent parti de différentes combinaisons d'éléments techniques, parfois aussi de contrats juridiques intelligents, avec l'objectif commun de donner à leurs utilisateurs davantage de transparence et de contrôle sur leurs données personnelles.

Il est certain que de nouvelles interfaces techniques sont nécessaires pour concrétiser le droit à la portabilité prévu aux articles 3 à 7 de la proposition de loi sur les données ». Ce régime exige en effet que les individus fassent preuve d'initiative personnelle pour invoquer ce nouveau droit à l'autodétermination informationnelle. Or, l'expérience acquise jusqu'à présent dans le cadre de la législation européenne sur les données, notamment en ce qui concerne le droit à la portabilité des données à caractère personnel prévu à l'article 20 du RGPD, a montré que les personnes ne prennent que rarement une telle initiative en ce qui concerne leurs données. Des outils techniques tels que le PIMS pourraient rendre les processus connexes plus efficaces et plus transparents afin d'abaisser les barrières existantes à l'initiative personnelle. Si l'on considère que cela profite directement aux utilisateurs de données, y compris aux personnes concernées, et leur donne plus de transparence et de contrôle pratique sur le traitement des données à caractère personnel qui les concernent, cela contribuerait également à atteindre les objectifs sous-jacents de la proposition de loi sur les données, à savoir accroître l'accès et le partage des données. Cela pourrait à son tour stimuler les innovations liées aux données et accroître la compétitivité du marché intérieur.

Au moment de la rédaction du présent rapport, les PIMS sont encore une catégorie naissante dont les structures, les modèles économiques et les supports techniques varient. L'étude fournit un aperçu des différentes caractéristiques des PIMS, telles que leurs modèles économiques, le stockage des données, la conception technique et les services offerts, et souligne les défis et les limites auxquels ils sont encore confrontés.

L'étude confirme que les PIMS utilisant des contrats juridiques intelligents peuvent faciliter la conclusion d'un contrat entre le détenteur et l'utilisateur des données et qu'ils peuvent être des outils utiles pour permettre l'accès aux données après une simple demande par voie électronique. L'étude constate également que les PIMS peuvent permettre aux utilisateurs de données de vérifier facilement leur propre identité et faciliter la gestion des informations sur les utilisateurs par les détenteurs de données. En outre, les PIMS peuvent également aider à déterminer la finalité du traitement des données à caractère personnel, et assurer le respect du régime du RGPD sur les droits des personnes concernées et le principe de transparence en vertu du RGPD.

Les contrats juridiques intelligents sont particulièrement utiles en vertu des articles 3 à 5 de la proposition de règlement « Loi sur les données », qui prévoit des relations contractuelles entre toutes les parties, car ils peuvent automatiser la conclusion et l'exécution de ces contrats sous réserve des limites identifiées par l'analyse comparative du droit civil dans la présente étude et, partant, réduire les coûts associés au partage des données.

Les PIMS utilisant des contrats juridiques intelligents doivent veiller à respecter les différentes exigences juridiques prévues par la proposition de règlement « Loi sur les données » et ils doivent en outre être conçus pour tenir compte des différents intérêts, notamment ceux du consommateur et du professionnel lorsque le droit de la protection des consommateurs est applicable, ainsi que les intérêts respectifs de la personne concernée et du responsable du traitement des données.

L'étude propose deux outils susceptibles de répondre à certaines de ces préoccupations : l'interopérabilité (sous quelques réserves) et les clauses contractuelles types. Ces deux outils pourraient, d'une part, encourager la prolifération de PIMS appropriés utilisant des contrats juridiques intelligents dans le marché unique numérique et, d'autre part, rendre plus attrayant pour les acteurs concernés de s'appuyer sur des PIMS utilisant des contrats intelligents.

List of abbreviations

Acronyms / Abbreviations	Definition
AES	Advanced Electronic Signature
AGID	Agency for Digital Italy
AISBL	Gaia-X Association for Data and Cloud
AI	Artificial Intelligence
ALC	Application Logic Contract
AML	Anti-money laundering
API	Application Programming Interface
AWS	Amazon Web Services
B2B	Business to Business
B2C	Business to Consumer
BI	Business Intelligence
BNT	Bancor Network Token
BSC	Binance Smart Chain
BR	Better Regulation (guidelines and toolbox)
BRIS	Business Registers Interconnection System
CAD	Italian Code of Digital Administration
CENELEC	European Committee for Electrotechnical Standardization
CISG	United Nations Convention on Contracts for the International Sale of Goods
CJEU	Court of Justice of the European Union
CPMI	Committee on Payment and Market Infrastructures
CRD	Consumer Rights Directive
CtD	Compute-to-Data
DA	Data Intermediary
DAML	Digital Asset Modeling Language
DAO	Decentralized Autonomous Organizations
DeFi	Decentralised Finance
DEX	Decentralised exchange
DFF	Dubai Future Foundation
DG FISMA	DG for Financial Stability, Financial Services and Capital Markets Union
DG JUST	DG Justice and Consumers
DID	Decentralized Identifier
DIFC	Dubai international Financial Centre
DINO	Decentralised in Name Only
DLT	Distributed Ledger Technology
DSL	Domain Specific Language
EBA	European Banking Authority
EBSI	European Blockchain Services Infrastructure
EC	European Commission

ECHR	European Convention on Human Rights
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EFTA	European Free Trade Association
ENISA	European Union Agency for Cybersecurity
ENS	Ethereum Name Service
ERC	Ethereum Request for Comment
ERP	Enterprise Resource Planning
ESBI	European Blockchain Services Infrastructure
ESMA	European Securities and Markets Authority
ESSIF	European Self-Sovereign Identity Framework
ETEK	Cyprus Technical and Scientific Chamber
ETH	Ethereum
ETSI	European Telecommunications Standards Institute
EU	European Union
EUBOF	EU Blockchain Observatory and Forum
EUCS	European Cloud Scheme
EUID	European Unique Identifier
EUR	Euro
EV	Extended Validation
EVM	Ethereum Virtual Machine
EWC	Energy Web Chain
FMI	Financial Market Infrastructure
FRAND	Fair, Reasonable and Non-discriminatory
FWC	Framework Contract
GCP	Google Cloud Platform
GDPR	General Data Protection Regulation
GLEIF	Global Legal Entity Identifier
GUnet	Greek Universities network
GVA	Gross Value Added
GXFS	Gaia-X Federation Services
HIPAA	US Health Insurance Portability and Accountability Act of 1996
IA	Impact Assessment
INATBA	International Association for Trusted Blockchain Applications
IOSCO	International Organisation of Securities Commissions
IoT	Internet of Things
IP	Intellectual Property
IPFS	InterPlanetary File System
ISO	International Organisation for Standardisation
IT	Information Technology
ITA	Innovative Technology Arrangement
JSON	JavaScript Object Notation
JTB	Joint Technical Body

JWT	JavaScript Object Notation Web Token
KID	Key Information Document
KYB	Know Your Business
KYC	Know Your Customer
LD	Linked Data
LEI	Legal Entity Identifier
MDIA	Malta Digital Innovation Authority
ML	Machine Learning
MNGO	Mango Token
MS	Member States
MVP	Minimum Viable Product
NAICS	North American Industry Classification System
NFT	Non-fungible token
NIST	US National Institute of Standards and Technology
ODRL	Open Digital Rights Language
PBFT	Proof-of-Byzantine-Fault Tolerance
PCI	Payment Card Industry
PDM	Personal Data Management
PDS	Public Distribution System
PFMI	Principles for Financial Market Infrastructures
PII	Personally Identifiable Information
PIMS	Personal Information Management Systems
PoS	Proof-of-Stake
PoSIs	Staking Infrastructure Providers
PoW	Proof-of-Work
PRIIPS	Packaged Retail and Insurance-Based Investment Products
PRLD	Policy Rules and Labelling Document
Q&A	Questions and answers
QES	Qualified electronic signature
QTSP	Qualified Trust Service Providers
RDF	Resource Description Framework
REA	Rapid Evidence Assessment
RON	Romanian Leu
SALSA	Self-assessed licenses sold at auction
SBS	Small Business Standards
SBT	SoulBound Token
SCS	Sovereign Cloud Stack
SES	SecureEcmaScript
SMEs	Small and Medium Enterprises
SOC	Service Organization Control
SOTA	Software-over-the-Air
SSI	Self-Sovereign Identity
SSL	Secured Sockets Layer

SSMI	Self-Sovereign Machine Identity
SST	Single Source of Truth
TSP	Trust Service Provider
TTP	Trusted third party
TVL	Total Value Locked
UCPD	Unfair Commercial Practices Directive
UCTD	Unfair Contract Terms Directive
USD	US Dollar
VC	Verifiable Credentials
VIEP	VAT Information Exchange System
WRC	Worldcore
ZKP	Zero-Knowledge Proof
zk-SNARK	Zero-Knowledge Succinct Non-interact Argument of Knowledge
zk-STARK	Zero-Knowledge Scalable Transparent Arguments of Knowledge

Common terms

Terms	Definition
Active validator set	The active validator set refers to all validators of a network who are currently authorized to engage in the validation process.
51% Attack	A 51% attack occurs if a single node or colluding nodes control more than 51% of the network. This would result in these nodes controlling who composes and validates new blocks.
Application Logic Contract (ALC)	Application Logic Contracts are designed to overcome the scalability drawbacks of traditional Internet of Things (IoT) architecture which relies on centralization. ALCs allow for secure device function alongside autonomous, scalable and cheaper transactions. They both communicate with and validate communication between different IoT devices further allowing them to oversee micropayments.
Blockchain Oracle	Device, entity or system which connects a deterministic blockchain to off-chain data.
Block explorer	Website linked to a public blockchain or distributed ledger that makes the entire history of the ledger visible and searchable for anyone with a web browser.
Burn Address	Digital wallet that cannot be accessed because it lacks a corresponding private key.
Certainty	The quality of being reliably true insofar as the settlement of a transaction can be concerned with respect to economic finality when taken at face value by a regulator.
Certain economic finality	Verifier's 'total skin in the game' is so high that no market participant would ever coax a verifier into reversing a transaction. Transactions are considered economically final once a supervisor can take them at face value.
Challenge	A potential obstacle that may prevent the use of a smart contract in the internal market and/or a rule that is not easily compatible with the smart contracts technology.
Consensus algorithm	Set of processes that define how nodes of a decentralized network can reach consensus on the current state of the network.
@context	@context elements are part of the JSON-LD format (described below). They provide more information which lets a computer interpret the rest of the data in greater depth and detail.
Compute-to-Data (CtD)	CtD enables data owners to grant only compute access to their data without the need to create copies in other environments they do not control. The data itself can remain with the data owner in a secured environment to minimize the risk of data-leaks.
Data Non-Fungible Token	Non-fungible ERC721 tokens which comprise the base intellectual property (IP) (equivalent to a master tape in music).
Data Token	Fungible ERC20 token representing data as the underlying tokenized asset.

Decentralized Finance (DeFi)	Decentralized finance is an umbrella term for an emerging set of technologies facilitating peer-to-peer transactions on public blockchains. DeFi allows for many processes and products that mirror traditional banking such as lending, earning interest, borrowing and trading assets. It relies on smart contracts which are, *for the time being*, mainly deployed on-top of distributed ledgers such as Ethereum, Solana, Avalanche, Polygon and as of 2021 also Bitcoin after the Taproot upgrade.
Decentralized Identifier (DID)	New type of identifier enabling verifiable, decentralized digital identity. A DID can refer to any subject (person, organization, thing, data model, artifact) as determined by the controller of the DID. They are designed so they can decouple from centralized registries, identity providers, and certificate authorities. Controllers of DIDs can prove control over it without requiring external permissions from third parties.
Decentralized network	In computing terms, a decentralized network distributes the given workload among multiple machines rather than relying on a centralized server or database. A decentralized network in the context of blockchain refers to the single source of truth (SST) of the data shared by all participants as the central point whereas the distributed computing among different machines is decentralized.
Decoupled Hashing	A hash gets computed for input variable and input value combinations of Person B's data with the compute running adjacent to the data. Hashing will anonymize the data and Person A then downloads the hashed data to train the model client-side.
DID Document	A set of data describing the DID subject, which includes mechanisms like cryptographic public keys that the DID subject or a DID delegate can use to authenticate itself and prove a corresponding association with the DID. A DID document could have one or many different representations.
Differential Privacy	Person B has sufficient random noise added to their data set for it to qualify as anonymized. Person A then downloads the partly-randomized data and trains the model client side.
Distributed Ledger Technology (DLT)	A distributed ledger technology or 'DLT' means a technology that enables the operation and use of distributed ledgers. Distributed ledger' means an information repository that keeps records of transactions and that is shared across, and synchronised between, a set of DLT network nodes using a consensus mechanism.
Domain Specific Language (DSL)	A computer language that is specialized to a particular application domain.
Economic impact	The effect of a policy or other activity meant to achieve a change in economic outcomes. Common outcomes of interest are Gross Value Added (GVA), employment, costs, prices, etc.
Electronic contract	An electronic contract is a legally binding agreement between at least two parties that is formed using electronic means.

ERC-20 Token	ERC stands for Ethereum Request for Comment and was introduced in 2015. ERC20 is the standard used for creating and issuing fungible smart contracts on the Ethereum blockchain.
ERC-721 Token	ERC stands for Ethereum Request for Comment and was introduced in 2015. ERC721 is the standard used for creating and issuing non-fungible smart contracts on the Ethereum blockchain.
Efficiency	A situation where the output of a production process (e.g., of a machine) cannot be increased without increasing at least one of its inputs; more specifically, "economic efficiency" then refers to the situation where an output cannot be increased without incurring an increase in the cost of production no matter how the factors of production are rearranged. In terms of analysis of efficiency, it will cover aspects of simplification (e.g., tackling inconsistencies) as well as potential of burden reduction (e.g., administrative costs).[9]
Embedded supervision	A conceptual regulatory framework that allows for compliance via automatic monitoring of decentralized markets by reading the state of the ledger supporting a given market that makes use of smart contracts. It is designed such that limiting the scale inherent in decentralized exchange could be overcome by having applications running on 'permissioned' DLT and peer-to-peer exchange facilitated by decentralized economic consensus. The use of on-chain data would then replace intermediary based legal data verification. Embedded supervision presupposes exchange between regulated entities and is considered in the context of an entity-based regulatory framework (i.e., the relationship between the underlying asset and the digital token must be guaranteed by the legal system).
Ethereum Name Service (ENS)	Distributed, open, and extensible naming system based on the Ethereum blockchain.
Ethereum Virtual Machine (EVM)	The environment in which all Ethereum accounts and smart contracts reside. At any given block in the chain, there is only one 'canonical state' and the EVM is what defines the rules for computing a new valid state from block to block.
Federated Learning	Learn a model across multiple data silos where compute running adjacent to the model is not for training purposes but for another purpose.
Fork(s)	In a blockchain, forks can be defined as the moment a blockchain diverges into two different paths forward. This could be either due to a change at the protocol level, or the point at which two or more blocks reach the same block height. They refer to additional instantiation(s) of a live network.

[9] European Commission, *Better Regulation Guidelines*, 2021. Available at: https://commission.europa.eu/document/d0bbd77f-bee5-4ee5-b5c4-6110c7605476_en.

Fungible Token	Representations of assets on the blockchain which are interchangeable and ‘exist more than once.’ The most common form of fungible token is a cryptocurrency.
Hard Fork	A backwards incompatible network software upgrade. Blocks created by nodes on the new protocol (post fork) are considered invalid by nodes on the old protocol (pre fork). These cause a chain-split.
JavaScript Object Notation (JSON) File	An open standard file/data exchange format which uses human-readable text to store and transmit data objects consisting of attribute-value pairs and arrays. It is a common data format with multiple uses within electronic data exchange and in web applications with servers.
JSON-LD	A JSON-based format to serialize Linked Data. The syntax is designed to easily integrate into deployed systems that already use JSON, and provides a smooth upgrade path from JSON to JSON-LD.
Kill Switch	In an IT context, kill switches can be understood as a mechanism used to shut down a device or program. For the purpose of this study, a kill switch refers to the ability to intervene in a smart contract and halt/reverse a given programmable function for the purpose of changing the outcome of the smart contract in effect circumscribing its immutability.
Label Issuer	In the Gaia-X Label Framework, Label Issuers comprise entities which are defined by the Gaia-X Association as able to implement and issue a label. Implementing a label brings all label requirements into the Verifiable credentials which then get encoded into the Compliance and Labelling Framework. A Label Issuer can be either Gaia-X or another AISBL verified issuer.
Label Owner	In the Gaia-X Label Framework, Label Owners comprise entities which seek to define a specific label for their business. These can include (but not limited to) service providers, service users, governmental authorities, standardization authorities, trade associations, industrial associations and others.
Legal Finality	Traditionally, legal finality refers to the discharge of an obligation where a transfer of funds for a transfer of securities have become both irrevocable and unconditional. For the purpose of this study, it can also be taken to include the legal finality of (a claim to/proof of ownership of) digital assets or other digital assets or fiat currencies and stablecoins within the context of a decentralized finance (DeFi) setting.
Measure	In this study, a measure is to be understood as normative acts issued by a competent Member State body (including EEA countries[10]), which is explicitly or implicitly mandatory in nature and

[10] Law Insider, Definition of ‘measure’, Available at: https://www.lawinsider.com/dictionary/measure.

	intends to produce legal effects[11] and which establishes or amends a rule in a way that may create or pose an obstacle to the existence or uptake of smart contracts.
NIST	The National Institute of Standards and Technology is an agency of the United States Department of Commerce with the goal of promoting American Innovation and industrial competitiveness. They are responsible for promoting industry standards related to operational and cyber resilience, cloud infrastructure and data governance.
NIST Cloud Federation Reference Architecture	An eleven-component model developed by the National Institute of Standards and Technology of the United States to define actor/agent relationships within a federated cloud infrastructure that can be deployed in public/private partnerships.
Nodes	The computers/servers that interact with the network via default or custom clients. There are different kinds of nodes with different roles, such as archival nodes (storing the full history of the blockchain), consensus nodes (validating new blocks added to the blockchain) or seed nodes (storing network addresses to connect nodes to each other).
Nonce	Nonce is an abbreviation for 'number only used once' and refers to the total number of confirmed transactions sent from a given wallet address.
Non-Fungible Token (NFT)	A unique digital identifier that cannot be copied, substitute or subdivided and effectively exists once. It is recorded in a blockchain and is used to verify authenticity and ownership.
Nothing-at-Stake Problem	The nothing-at-stake problem is a phenomenon that occurs when the validating nodes in a protocol can generate and maintain multiple forks at no cost.
Obstacle	An obstacle is to be understood as a diverging mandatory measure in a Member State, which has the effect of preventing or hindering fundamental freedoms or distorting competition within the internal market.[12] An obstacle for smart contracts - for the purpose of this study - is a diverging mandatory measure (typically private law rule) that actually prevents or hinders the uptake and roll-out of smart contracts within the internal market.
Open Digital Rights Language (ODRL)	A policy expression language that provides a flexible and interoperable information model, vocabulary, and encoding mechanisms for representing statements about the usage of content and services.
Personal data management tool	Products and services that help individuals to have more control over their personal data.

[11] Order of the General Court T-192/16 – NF v European Council.

[12] Case C-376/98 – Germany v Parliament and Council (*Tobacco advertisement judgment*).

Personal Data	Any representation of information which allows for inferring the identity of an individual based on either direct or indirect means Article 4(1) GDPR defines personal data as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
PoS (Proof-of-Stake), PoW (Proof-of-Work), Proof-of-X	Processes to appoint the node which gets to create the next block.
Private law rule	A measure that defines, regulates, enforces, and administers relationships among natural and legal persons.[13] In the course of this study, such rules mainly include rules of civil law (e.g., civil code) but are not limited to these rules (e.g., lex specialis in consumer protection law).
Probabilistic settlement	Transaction validation via nodes converges to but never reaches zero and with time slip under certain consensus mechanisms or due to a fork, revocation can occur. Therefore, with probabilistic settlement, although the legal framework (including in the case of a stablecoin arrangement – its own rules) can define the point of legal finality, technical settlement may never be guaranteed with absolute certainty. Conclusiveness of the state of the ledger is proportional to the number of transactions, which get added to it. However, settlement risk implications from a fork also increase concurrently with the number of transactions.
Reverse transaction	The ability to cancel or reverse a pending transaction on a smart contract.
Rug Pull	A type of cryptocurrency scam where developers attract investors but disappear before the project is finished; selling their tokens and leaving investors with worthless assets and losses.
Self-assessed licenses sold at auction (SALSA)	A use-case possible through SoulBound Tokens. Asset holders can post a self-assessed price for anyone else to purchase their asset from them. A periodic tax proportional to the self-assessed price must be paid to maintain control.
Single Source of Truth (SST)	A network of computers or nodes where each node stores the same information. A blockchain can contain the same information on each node. The SST is what underpins the built-in trustlessness of consensus to operate.
Slashing	In the case of validator misbehaviour (defined individually within each protocol), the total stake of the validator (Own Stake/security deposits and sometimes even delegated stake) gets slashed,

[13] Collins Dictionary of Law, 2006. Available at: Private law legal definition of private law (thefreedictionary.com).

	meaning that a certain percentage of tokens is burned and distributed to the treasury. This is designed to incentivize security, availability of governance participation as well as prevent double-spend or spam attacks.
Smart contract (based on DLT/blockchain)	Smart contracts are programmable lines of code (if x then y statements), automatically executing such actions as initiation, verification, execution and enforcement of terms and conditions so long as certain pre-determined criteria within their coding is met. They allow for transaction engagement between two or multiple transparent, pseudo-anonymous or fully anonymous parties. For the purpose of this study several different forms of smart contracts supporting different 'use cases' can be understood, including time-lock contracts, application logic contracts and smart legal contracts.
Smart Legal Contract	A legally binding contract in which, either some or all of the associated terms, conditions and rights under the contract are defined in and/or performed by code execution.
Soft Fork	A backwards compatible network software upgrade. Nodes that are the old protocol (pre fork) consider blocks created by nodes on the new protocol (post fork) valid. Blocks created by nodes on the old protocol (pre fork) may not be considered valid by nodes on the new protocol (post fork) though. These do not cause a chain-split.
SoulBound Token	Non-fungible, non-transferable, and public-verifiable digital tokens. They can be used for immutable records such as employment history, work experience, and academic credentials. SoulBound Tokens act as a 'Proof-of-Knowledge.' They expand the utility of Non-Fungible Tokens.
Staking Infrastructure Providers (PoSIs)	PoSIs are specific nodes that provide the technical infrastructure and maintenance required by the respective network. In addition, PoSIs provide services such as acting upon voting and validation rights. PoSIs hold these rights either through delegation by their clients and/or through their own token holdings.
Sybil Attack	A sybil attack happens in case one participant of the network creates multiple nodes in order to gain an absolute majority of the network's voting power.
Time Lock Contract	Time locked contracts consist of digital assets that are deposited and 'locked' for a pre-determined period before the sender can retrieve them. They consist of a time-lock function or a numerical timestamp for each deposit address. Tokens can only be withdrawn to a given address once their associated timestamp expires. Prior to this the lock contract only accepts deposits.
Tokenisation	The process of representing programmable assets or access rights that have been digitalized. Tokenized assets that are represented on a blockchain can conversely be used, owned, and transferred without the need for a third-party intermediary.
Transaction Fee	When using decentralized networks, the process of initiating transaction transfers incurred fees levied onto the user. These fees

	prevent the network from being spammed and are used to compensate validators for their work.
Trust Anchor	Entities which are endorsed by Gaia-X. Trust anchors facilitate claims processing by participants under the Gaia-X Trust Framework. Compliance under the Trust Framework requires all key pairs used to sign claims having at least one Trust Anchor in their certificate chain. At any point in time, the list of valid Trust Anchors is stored in the Gaia-X Registry.
Validator	Validators are special nodes in PoS based networks. They provide the technical infrastructure and maintenance required by the respective network. Validators propose and validate new blocks and actively participate in the network's governance by either submitting or voting on new proposals (depending on the network).
Web3	An emergent term for a new classification of the World Wide Web based on concepts such as decentralisation, blockchain technology and token-based economics.
WRC Verifiable Credentials	A tamper-evident credential that has authorship which can be cryptographically verified.
WRC Verifiable Presentations	Can express data from one or more verifiable credentials while being constructed in a way that the authorship of the data is also verifiable. A holder can select given pieces of information to compose into a new context specific presentation of personal data. This newly created composite proof can be sent to the verifier to validate its legitimacy.
ZKP	Stands for Zero-Knowledge Proof. A cryptographic proof where verifying the proof is possible without revealing what is being verified.
zk-SNARK	Stands for Zero-Knowledge Succinct Non-interact Argument of Knowledge. A cryptographic proof where verifying the proof is possible without revealing what is being verified and without any interaction between the prover and the verifier.
zk-STARK	Stands for Zero-Knowledge Scalable Transparent Arguments of Knowledge. It refers to a form of cryptographic proof that allows users to share either validated data or perform computations with a third-party without revealing the data and/or computation to the third party.

1. Introduction

1.1 Study objectives and scope

This document presents the final report for the study on civil law rules applicable to smart contracts, under DG JUST's Framework Contract JUST/2020/PR/03/0001 for Evaluation, Impact Assessment and Related Policy Support Services in the Justice and Consumers Policy Areas. The report sets out the final findings and conclusions from the data collection and analysis conducted by VVA Brussels, LE Europe, Datarella, and Prof. Michèle Finck.

The objective of the study was to assess the legal, economic and technical feasibility of implementing smart contracts within the European Economic Area (EEA), both in Business to Business (B2B) and Business to Consumer (B2C) relations. The study aimed to provide information on existing obstacles caused by country measures for the use of smart contracts based on distributed ledger technology (DLT), including the extent and the economic context of these problems, through legal and economic analysis. Furthermore, two other core objectives of the study were to give an overview of possible technical solutions applied to smart contracts, as well as to provide an assessment of the overall potential of DLT and smart contracts in terms of data sharing, particularly by personal data management tools.

This study covered the 27 EU Member States, as well as Liechtenstein, Iceland, and Norway. Hereafter, all 30 EEA countries are referred to as EEA Member States.

In line with the tender specifications, this study used the notion of smart contracts as a broad category which, inter alia, also includes smart legal contracts (please refer to the Common terms above). This terminology gives the opportunity for flexibility and adjustment in a dynamically evolving policy field and thus contributes to the durability of the analysis. Notwithstanding, these terminological choices should not hide the fact that only a part of existing smart contracts are relevant from the perspective of contract law. To render this distinction more tangible, references to certain types of smart contracts are provided as examples throughout the text.

1.2. Structure of the report

This report is structured as follows:

- **Chapter 1** provides the key objectives and scope of the study.
- **Chapter 2** provides an overview of the methodology applied.
- **Chapter 3** presents the study findings and is divided into sections on the economic features of smart contracts, the comparative law analysis, the technical feasibility assessment and the analysis of personal data management tools based on DLT.
- **Chapter 4** summarises the study conclusions.
- **Annex I** presents the questionnaire template for national legal research.
- **Annex II** provides an analysis of the impact of smart contracts based on DLT.
- **Annex III** presents a technical feasibility matrix.

2. Overview of the methodology

2.1. Economic features of smart contracts

In section 3.1 an economic assessment of the features of smart contracts in the context of the European economy was undertaken based on a review of relevant literature and data sources, interviews with market participants, and a theoretical appraisal of the economic characteristics of smart contracts and their implications for adoption in the EU. Given the lack of robust data on the value of the market for smart contracts and the available indications that current uptake is not economically significant, the study presents a set of stylised facts regarding the potential for impact in different settings.

2.2. Comparative law analysis

The legal research was carried out by our network of national legal experts (qualified lawyers and academics) and validated by the core legal team. The output of this task was 30 national reports covering all EEA Member States. The reports were based on a questionnaire consisting of 25 questions (see Annex I). It should be noted that the national legal experts based their answers on their own research and assessment, thus focussing on various aspects of the questions raised. Therefore, rules, examples and challenges and/or obstacles mentioned in certain EEA Member States might be relevant in other EEA Member States as well (even if they were not singled out specifically by the national experts in the national report).

The national legal research, in addition to finding out whether any legislation on smart contracts exists in the EEA Member States, covered the national provisions and relevant literature on contract formation, form requirements for contracts, contract interpretation and termination, as well as the application of consumer law requirements to smart contracts. Based on the findings of the national research on the abovementioned topics, a comparative analysis (section 3.2) was conducted and conclusions were drawn on the differences, as well as similarities, between national measures (i.e. the extent of differences among national rules). Besides, the analysis examined the issue of legal (un)certainty and investigated whether the identified national measures applicable to smart contracts may constitute obstacles to the roll-out of smart contracts in the EU. It also identified national and/or EU rules that may be difficult to comply with due to the nature of the smart contracts technology.

2.3. Technical feasibility assessment

The technical feasibility assessment (section 3.3) combines the main findings from the legal desk research and creates a path for understanding the feasibility of applying technical solutions to the challenges identified. In this context, the assessment further draws on three case studies covering smart contract applications in the following contexts: deltaDAO AG, CashOnLedger and Bosch. On this basis, a feasibility matrix (Annex III to this report) was developed to provide further visual information on defined challenges and their technical solutions.

The ‘Techno Economic implications’ sub-section (3.3.2) is divided into an analysis of identified technical measures for (i) infrastructure, security and consumer protection and (ii) data portability and decentralised identity. Based on commonly identified themes, the main techno-economic implications centred on reverse transaction features, safe termination, embedded supervision, alongside different decentralised identity schemas including W3C Verifiable Credentials, SoulBound Tokens and Zero-Knowledge Proof cryptography. The overarching technical ‘themes’ were distilled as the main applied aspects of the previous desk research.

Therefore, the analysis of techno-economic implications takes a broader, applied view from a market perspective. This was contrasted against the impact of EU legislation on smart contracts defined under the draft Data Act, including the potential future impact of the Data Act on public permissionless blockchains. Where possible, quantitative examples were used to support categorical findings related to the use of different technical measures. The sub-section closes with a stock taking of each of the identified measures including overarching policy recommendations for their application.

2.4. Analysis on personal data management tools

In section 3.4, the study provides a comprehensive analysis of the potential of DLT and smart legal contracts to facilitate access to and sharing of personal data, specifically in respect of personal data management tools. It builds on the more general comparative legal analysis, as well as the technical analysis. Whereas these analyses evaluated smart legal contracts more generally, the analysis of Personal Information Management Systems (PIMS) is concerned with a very specific application of smart legal contracts, namely how they relate to the specific use case of personal data management tools. The analysis touches on the current state of informational self-determination, meaning the ability of individuals to control data related to them in the online environment and explains the EU legislature’s intention to increase access to and sharing of data, inter alia through the draft Data Act’s new data portability mechanism for IoT devices.

In this context, the analysis introduces PIMS and their main features. Based on desk research, as well as interviews with relevant stakeholders, the various features of PIMS are introduced and examined specifically in the context of the extent to which smart contracts are deemed to be important components of these systems, both from a theoretical and practical perspective. In addition, the analysis determines what design requirements compliant PIMS using smart contracts would need to respect with reference to the most relevant provisions of the General Data Protection Regulation (GDPR) and the draft Data Act.

Finally, the analysis determines, on the basis of desk research as well as the outcome of industry interviews, how the design of PIMS using smart legal contracts can account for different interests, particularly those of the data holder, the data user and the third party under the draft Data Act; as well as those of the data controller and the data subject under data protection law; and between the consumer and the trader in consumer protection law. The analysis closes with two overarching policy recommendations on interoperability and model contractual terms.

3. Study findings

3.1. Economic analysis of smart contracts

This section discusses the potential economic features of smart contracts based on DLT. The section is based on desk research and expert interviews. Overall, the available literature, verified by our interviewees, indicates that there are a broad range of potential applications for smart contracts, but with relatively limited current take-up.[14] In a broad sense, smart contracts can be seen as another step towards greater process automation and efficiency enhancement with near-universal applications in B2B and B2C transactions. However, existing use cases are mostly small and confined to niche applications with unproven business models. The benefits and costs of smart contracts at the economy level are therefore almost impossible to quantify.

Nonetheless, a few stylised facts can be identified based on the research for this study.

Direct benefits of smart contracts include:

- **Automation**: smart contracts can automate increasingly complex transactions (although in some cases, complete automation, while technically feasible, is undesirable, e.g., in the case of B2C transactions, where 'human-in-the-loop' models are preferred by users and are sometimes mandatory). This can result in:
  - Reduced costs of human labour;[15]
  - Increased transaction speeds.
- **Security**: Smart contracts make use of encryption at the blockchain level and are fully auditable.
- **Disintermediation**: In many applications, smart contracts can eliminate the need for intermediaries, thereby reducing transaction costs. However, the DLT network and technology providers are new classes of intermediaries that represent new cost factors. While this new type of intermediation (including from DLT startups) can be value added, it involves a new cost to parties who were previously transacting bilaterally.
- **Accuracy**: The transaction process is less error prone, leading to reduced execution risk; this has second-order benefits through reduced costs of compliance and complaints handling systems, reduced insurance premiums, reduced litigation costs, fines, damages etc.

[14] See Annex II for a discussion on measurement of smart contract use and economic impact.

[15] A case study of a smart contract application in the AaaS space (Cash On Ledger, see also Task 3) mentions a reduction in labour cost per unit of output of one third (see https://cash-on-ledger.com/fully-automatic/). A report (GSMA, 2021) on the use of blockchain-based smart contracts for wholesale roaming estimates that the solution "can reduce the time required for a settlement from 1 day on average to probably 30 minutes in the beginning and 10-15 minutes when fully operational with all roaming partners which is 1/30th of the initial time required." (https://www.gsma.com/services/blog/how-blockchain-can-speed-up-inter-operator-settlement/, p. 28).

- **Trust**: To the extent that smart contracts generate greater trust between parties, more transactions take place, and the cost of alternative trust-building/preserving measures is reduced.

On the cost side, market participants perceive set up costs as high. There is currently a mismatch between the cost of the infrastructure (including initial setup) and the direct benefit to users of the technology. Venture capital investment in technology providers helps to bridge this gap, but sustainability will require a scale of adoption that is currently elusive. Per-transaction costs for smart contracts that use DLT networks are higher than for traditional database solutions. Operating the nodes in a DLT network requires computation, data storage, transfer infrastructure and operating expenses, as well as technical expertise that is currently already in short supply.

The legal analysis has identified the cost of changing a smart contract as a significant concern.

In addition, smart contract business models often use complex pricing models based on more detailed data on the underlying transaction, which is arguably a key advantage, but could be an obstacle in industries used to simpler pricing models. At the moment, the perception – sometimes fuelled by the industry – is that considerable technical expertise is needed to set up and operate smart contracts on the blockchain.

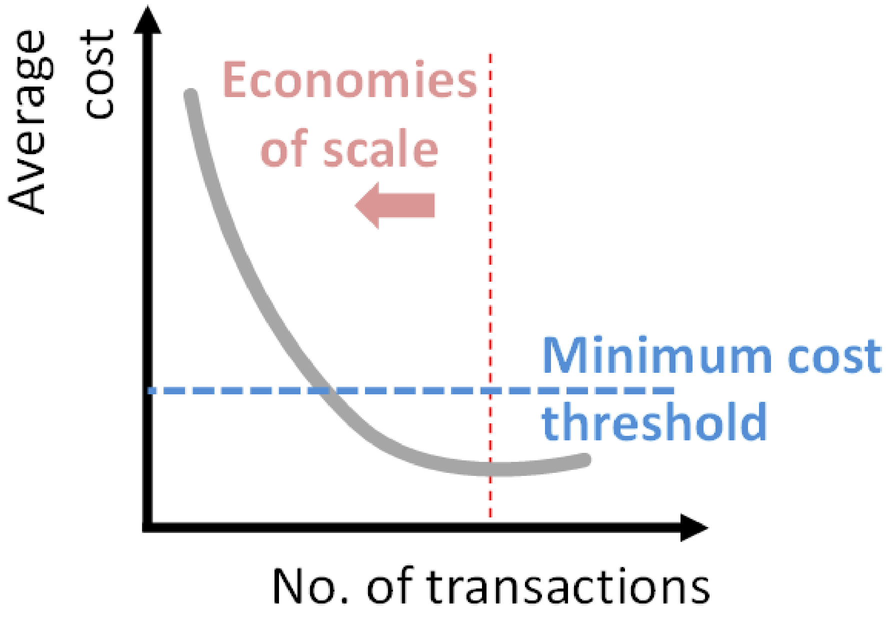
3.1.1. Implications for the market potential of smart contracts

One key to the success of smart contracts is realising economies of scale. The more transactions, the greater the sum of the per-transaction savings and the more the setup and operational costs can be spread out. The volume of transactions can come either through frequency (e.g., trade execution and settlement), from the number of parties involved (e.g., product recalls, class actions), or both. This suggests that larger entities (with lots of customers and/or lots of suppliers) or entities involved in markets with high transaction volume and frequency (such as financial services[16]) will be the first and biggest beneficiaries.

Moreover, B2B applications are more likely to benefit in the medium term, as consumer protection measures (e.g., right of withdrawal and information requirements for traders) present specific challenges for the use of smart contracts. Such challenges (i.e. any measures that increase the cost of implementing smart contract solutions) can be thought of as a minimum cost threshold (see graph below) that limits the potential cost savings from a smart contract for certain classes of transactions (for example, some use cases may require two separate smart contracts to ensure that transactions can be reversed if a consumer exercises their withdrawal right).

[16] The number of start-ups focusing on financial applications supports this view, see relevant section.

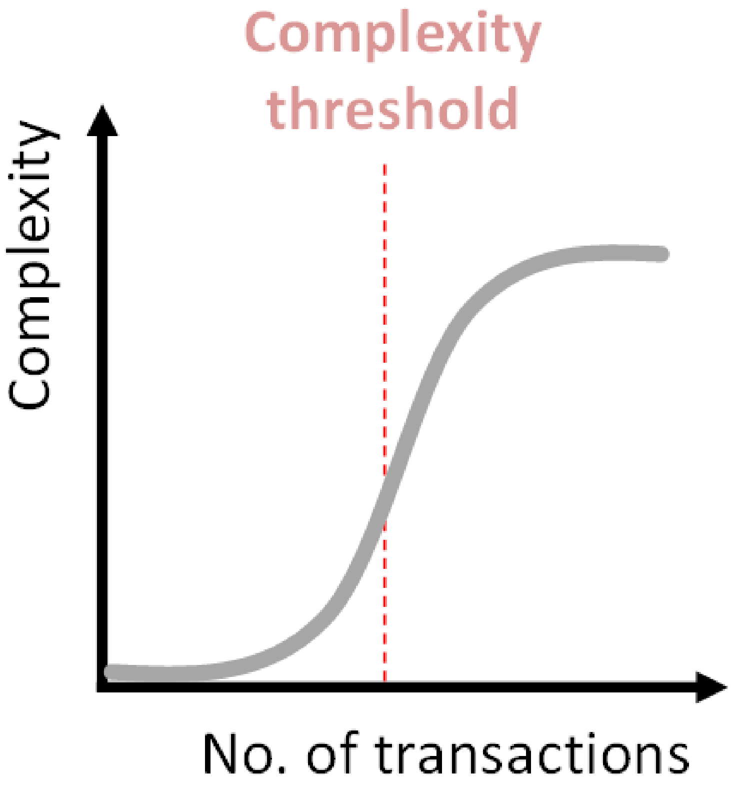
Figure 1: Economies of scale in smart contracts applications



Source: LE Europe

At the moment, the benefits of the economies of scale are not yet evident. At the same time, smart contracts work best for relatively simple cause-effect links (if this happens then this happens), while human input will for the time being remain important in more complex contractual relationships. One advantage of simple applications is that they are more auditable and comprehensible to humans, which makes their application less controversial. Other considerations such as development cost and resource intensity also favour simpler algorithms. It is thus likely that early smart contract applications sit on the lower end of a complexity spectrum that is unique for each use case, but likely has a generalisable shape (see figure below).

Figure 2: Complexity distribution in a smart contracts application



Source: LE Europe

The complexity threshold (below which smart contracts can replace current processes) may be expected to move to the right over time as technology becomes ‘smarter’.

In some applications, there may be important second order effects to consider. The key one being that reducing the cost of execution drives demand for the underlying transactions. This could be problematic in domains where the existing systems are not set up to handle increased transaction volumes. An example that has been cited by an interviewee is automated compliance with the proposed EU Data Act[17], where users have a right to access data created by their use of a connected device from the manufacturer. If this right was implemented as an automatically executable request in a smart contract, the amount of data that would therefore need to be shared could be immense. This scenario may pose a challenge to data holders that have so far experienced very few direct requests for data, which are typically addressed on a case-by-case basis. Similar applications, such as automated compensation in the case of consumer rights infringements, automated enrolment in class action lawsuits etc., have the potential to greatly increase the volume of transactions. Such diseconomies of scale may characterise many smart contract

[17] See section 3.4.**Error! Reference source not found.**

applications in the medium term, whilst the technical and regulatory support infrastructure develops.

The legal framework has a crucial role here: the more smart contracts affect business transactions and people's lives, the more the legal system will need to be able to deal with the review of smart contracts. The proliferation of different DLT networks and smart contract algorithms can present an extra challenge. One interviewee advocated for an EU level certification of permitted algorithms for smart contracts to reduce the burden on the judicial system.

On the plus side, more efficient resource utilisation enabled by smart contracts could in time reduce the overall environmental impact of economic activity, e.g., by optimising the use of tangible assets through DLT-enabled AaaS[18] business models (see Cash On Ledger example in section 3.3).

3.1.2. Effects on smaller firms

Another issue is to what extent smart contracts can change the competitive balance between smaller and larger businesses. The current system of traditional contracts can be seen to benefit larger companies that can afford expensive legal advice or hire in-house legal teams, more so than smaller companies who lack the resources to have full-time employees deliberating over contractual legalities. The introduction of smart contracts has the potential to reduce the marginal cost of scaling for smaller firms by reducing the need for 'lumpy' investments in capabilities to deal with contracting.

Smart contracts are designed so that there are minimal legal uncertainties and their automated execution eliminates some human error elements that can lead to contractual disputes. As such, smart contracts may help to avoid some litigation costs that would have occurred if traditional contracts had been used.

Not only may smart contracts provide an avenue for smaller companies to bridge the gap with larger companies' ability to navigate the law, but they may also reduce the marginal cost at which companies make contracts. Smart contracts can replace several traditional contracts with one smart contract which encompasses all the components of the deal, thereby reducing the need for labour costs of those presiding over the traditional contracts. Other benefits are detailed above, but it is clear to see how smart contracts may provide opportunities for small companies to increase their competitiveness.

However, evidence from Zolas et al. (2020)[19] shows that larger and older firms are more likely to adopt advanced technologies. It may be that larger European companies are those that are more willing to invest in smart contract technology more quickly than their smaller counterparts. Changes to the EU regulatory landscape, which allow for companies to adopt smart contracts more easily, may affect this balance.

3.1.3. Smart contracts and DLT

An important consideration, given the scope of this study, is the role of DLT for the benefit of smart contracts (the considerations above apply to smart contracts more broadly). Data

[18] Analytics as a Service.

[19] https://www.nber.org/papers/w28290.

aggregation and processing solutions that do not use DLT, generally, have cheaper running costs. The unique features of DLT, including transparency and built-in trust through verification, add value in certain applications, but are not necessary for many smart contracts.

Another important consideration for the overall benefit estimate is the role of payments: in transactions where money changes hands, another set of contracts to enable payment needs to be in place, increasing the potential benefit of smart contracts. However, the benefit may be further increased if payments stay within the smart contract ecosystem, i.e. use digital tokens that are only rarely converted into money (analogous to the relationship between inside and outside money).

3.1.4. Conclusions on economic features of smart contracts

Based on the market soundings and literature review undertaken for this study, smart contract adoption in the EU, at present, is negligible in terms of economic value. It was not possible to find evidence on the relevance of smart contracts in cross-border transactions in the EU.

The cost of current solutions is high, economic operation depends on a minimum efficient scale that is currently not achieved at the market level (profitable examples may exist at the enterprise level and in one-off projects).

The economic advantages of blockchain-based smart contracts are most likely to be present in high-volume markets (in terms of a large number of market participants, a large number of transactions, or both). Examples are financial services, data management, wholesale roaming.

B2B applications are more likely to see take-up as there are additional constraints and requirements for B2C contracts (arising from consumer protection objectives) that increase the complexity of smart contract solutions in this area. In addition, deployment is easier in markets where transaction complexity is low and where transactions stay on chain, with no requirement for frequent conversion to outside currency.

Many promising use cases for DLT-based smart contracts exist in economically important markets (financial services, data management, communication) and in important emergent technologies (autonomous systems, PIMS). However, the higher cost of DLT solutions compared with traditional data processing solutions have already caused some experiments with DLT solutions to be abandoned. Cross-border transactions may be assumed to be particularly attractive use cases because they replace especially costly contract solutions involving transnational legal issues, especially if transactions remain on chain, and the more so the lower the level of prevailing institutional trust transacting parties can rely on. However, this advantage is reduced if there remain substantially different national rules for smart contracts.

3.2. Comparative law analysis

This section contains a comparative analysis of the findings from the national legal research. It is divided into seven subsections with the first focusing on the existence of legislation on smart contracts and/or relating to the use of distributed ledger technologies across the EEA Member States. Afterwards, the rules on contract formation and form requirements in the EEA Member States are analysed before the section discusses the issue of contract interpretation/evidential value in this context. On this basis, an analysis of the civil and consumer law requirements, as well as requirements on termination of contracts and remedies is presented. Finally, this section concludes on the results of the comparative law analysis across the EEA Member States.

The comparative legal analysis provides a wide-ranging overview of existing rules and principles regarding contract law rules in EEA Member States. It also sheds light on challenges and obstacles smart contracts could face in the current legal environment across EEA Member States. However, it should be noted that due to the current low level of application of smart contracts in EEA Member States and to the small number of existing specific legislation on smart contracts, the comparative legal analysis has limitations in terms of coverage of rules specifically focused on smart contracts. It should be also borne in mind that rules, examples, and challenges mentioned in certain EEA Member States might be relevant in other EEA Member States as well (even if they are not specifically mentioned in the text). As such, the number of Member States where a certain rule exists is only indicative, and not exhaustive, in view of the methodology used for the legal analysis.[20]

3.2.1. Applicable legislation

Table 1 below provides an overview of the existence of legislation specifically enacted to apply to smart contracts and/or relating to the use of distributed ledger technologies (DLT) in all EEA Member States.[21] In this table, the symbol '✓' should be understood as indicating the presence of legislation, while the symbol '✘' should be interpreted as indicating the absence of legislation.

Table 1: Existing legislation on smart contracts and/or DLT

EEA Member State	Legislation on smart contracts and/or DLT
Austria	✘
Belgium	✘
Bulgaria	✘
Croatia	✘
Cyprus	✘
Czechia	✘
Denmark	✘
Estonia	✘

[20] The questionnaire template for the legal research can be found in Annex I.

[21] All 30 EEA countries are referred to as Member States.

Finland[22]	✓
France[23]	✓
Germany[24]	✓
Greece[25]	✓
Hungary	✗
Iceland	✗
Ireland	✗
Italy[26]	✓
Latvia	✗
Liechtenstein[27]	✓
Lithuania	✗
Luxembourg[28]	✓
Malta[29]	✓
Netherlands	✗
Norway	✗
Poland	✗
Portugal	✗
Romania	✗
Slovakia	✗
Slovenia	✗
Spain	✗
Sweden	✗

As can be seen from the table above, three EEA Member States have adopted legislation that contains definitions of both smart contracts and DLT **(GR, IT, MT)**, while five have legislation in force specifically on DLT (on its use in the financial sector) but not specifically

[22] Legislation on DLT.
[23] Legislation on DLT.
[24] Legislation on DLT.
[25] Legislation specifically on smart contracts.
[26] Legislation specifically on smart contracts.
[27] Legislation on DLT.
[28] Legislation on DLT.
[29] Legislation specifically on smart contracts.

on smart contracts **(DE[30], FI[31], FR[32], LI[33], LU[34])**. The remaining EEA Member States have no legislation in place specifically relating to the use of DLT and/or specifically applicable to smart contracts. However, it should be noted that the Government of **Cyprus** published a draft law on DLT in 2021 for public consultation, which included provisions (e.g., a definition) specifically on smart contracts (under Part IV).[35] Eventually, the government of Cyprus decided to abandon the draft law and it was not adopted.[36]

In **Greece**, the normative act[37] regulating smart contracts was passed in July 2022. The new legislation lays down the definition of smart contracts, which reads as follows: 'a smart contract is a set of coded computer operations, which is finalised and executed through distributed ledger technology in an automated electronic form by means of instructions to perform actions, omissions or tolerances, which are based on the existence or non-existence of certain conditions, in accordance with terms written directly into electronic code, programmed instructions, or programmed language'[38]. The Greek law contains rules on the conditions for the formation of smart contracts, and rules of validity and content. It also introduces provisions on the evidential value of smart contracts in civil procedure.

In **Italy**, the relevant legislation[39] was introduced in 2018. It contains specific rules for DLT and smart contracts, including definitions. According to the Italian act, a smart contract is 'a computer program that operates on technologies based on distributed registers and

[30] Law of 1 January 2020 on the Implementation of the Amending Directive to the Fourth EU Money Laundering Directive (Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie) regulates the crypto depository service (or crypto custody - Kryptoverwahrgeschäft), including fintech start-ups, established banks and foreign cryptocurrency exchanges. Another important piece of legislation is Law of 3 June 2021 on the introduction of electronic securities (Gesetz zur Einführung von elektronischen Wertpapieren). This law allows three types of securities – debt securities, bonds (Pfandbriefe) and investment unit certificates – to be issued electronically. In the regard of these electronic securities, the law differentiates between central register securities and crypto securities. Above that, based on electronic securities law, Regulation of 3 June 2022 on crypto shares (Verordnung über Kryptofondsanteile – KryptoFAV). allows to issue electronic fund shares via decentralised crypto securities registers (based on DLT).

[31] Act on Virtual Currency Providers (572/2019). The primary objective of this Act is to bring virtual currency providers under the scope of anti-money laundering regulation.

[32] Legislation on DLT encompasses the Order of 28 April 2016 for the transfer of mini-vouchers, which authorized the use of a shared electronic recording device. Furthermore, DLT legislation in France includes Order of 8 December 2017 on the authorisation of the use of a shared electronic recording device for financial securities not admitted to the operations of a central securities depository. Moreover, Decree No. 2018-1226 of 24 December 2018 on the use of a shared electronic registration device for the representation and transmission of financial securities and for the issuance and transfer of mini-bonds specifies the conditions applicable to the registration of financial securities on a blockchain.

[33] Blockchain Act of 2019 (Token- und VT-Dienstleister-Gesetz; TVTG). The main objective of the law is to provide certainty of rights for users and providers of DLT and to combat financial crimes in relation to DLT by enforcing due diligence duties on blockchain-based businesses.

[34] Law on Distributed Ledger Technology (2021 DLT Law). See also: https://www.bsp.lu/lu/publications/newsletters-newsflashes/law-distributed-ledger-technology-adopted.

[35] Bill entitled "The Distributed Ledger Technology Law of 2021". Article 2 of the draft law defines smart contracts as 'a set of coded computer functions with regards to crypto assets which is finalized and executed through DLT in an automated electronic or digital form through executable instructions for actions, omissions or tolerances, which are based on the occurrence or non-occurrence of specified conditions, according to terms which are recorded directly in codes, programming commands or programming language'.

[36] Cyprus Bar Association, Communication on the decision of the Ministry of Finance to withdraw the bill on "Distributed Ledger Technology Law"
Available at: https://www.cyprusbarassociation.org/index.php/en/news/32244-anakoinose-schetika-me-ten-apophase-tou-ypourgeiou-oikonomikon-gia-aposyrse-tou-nomoschediou-ypo-ton-titlo-o-peri-technologias-katanemenou-katholikou-nomos.

[37] Law 4961/2022 on Emerging Information and Telecommunications Technologies, enhancement of digital governance and others.

[38] Ibid.

[39] Law no. 12 of 11 February 2019 (Legge 11 febbraio 2019, n. 12, di conversione del decreto legge 14 dicembre 2018, n. 135, recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e la pubblica amministrazione), also called 'Simplification Decree' (Decreto Semplificazioni).

whose execution automatically binds two or more parties on the basis of effects predefined by them'[40]. The Italian Decree also lays down that:

- smart contracts satisfy the requirement of the written form, upon prior IT identification of the interested parties meeting the requirements of the Agency for Digital Italy (AgID), set out in its guidelines;
- the storage of an electronic document onto DLT has the legal effect of the electronic timestamp pursuant to the eIDAS Regulation;[41]
- the above legal effect comes into existence provided that the DLT meets the technical standards[42] which will be published by the AgID.

In **Malta**, three laws[43] were enacted in 2018 creating a legal framework for blockchain technology, encompassing rules on smart contracts. The definition of smart contracts in Maltese law is incorporated in the Malta Digital Innovation Authority Act,[44] which stipulates that: 'smart contracts, as a form of innovative technology arrangement, consist of a computer protocol and/or an agreement concluded wholly or partly in an electronic form, which is automatable and enforceable by execution of computer code, although some parts may require human input and control and which may be also enforceable by ordinary legal methods or by a mixture of both'.[45]

The findings do not indicate whether the legislation specifically applicable to smart contracts and/or relating to the use of DLT has had a positive or negative effect on the adoption of smart contracts in the Member States where such legislation exist. However, in **France**, smart contracts were used in the field of insurance law between 2017 and 2019,[46] for example for the automatic compensation of damage victims in case of delayed or cancelled flights, through the Fizzy platform launched by the French insurance company Axa.[47] Additionally, **Germany** plans to start applying smart contracts in the energy sector, which would be an occasion to increase the use of smart contracts in the country.[48]

Challenges

In the framework of this study, several challenges posed by existing measures at EEA Member State level were identified. These challenges may be linked to the legal uncertainties and difficulties to ensure compliance with applicable rules, which might eventually lead to an obstacle concerning the deployment and the use of this technology.

[40] Art. 8 par. 2 of Law no. 12 of 11 February 2019 (Simplification Decree).

[41] Article 41 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation).

[42] It should be noted that at the time of writing of this report, these technical standards are still not issued.

[43] 1) Malta Digital Innovation Authority Act (MDIA Act); 2) Innovative Technology Arrangements and Services Act (ITAS Act); 3) Virtual Financial Assets Act (VFA Act).

[44] Article 2 of Act No. XXXI of 2018 (Malta Digital Innovation Authority Act).

[45] Ibid.

[46] Axa decided to discontinue the use of smart contracts due to insufficient demand.

[47] Artificial Lawyer, 'AXA Scraps Fizzy Insurance Smart Contract…But Still Interested in the Tech', 2020. Available at: https://www.artificiallawyer.com/2020/10/08/axa-scraps-fizzy-insurance-smart-contract-but-still-interested-in-the-tech/.

[48] The Federal Government of Germany published its Blockchain Strategy in 2019 (available at: https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/blockchain-strategie.html), in which the set-up of a register for smart contracts in the energy sector was foreseen, which would enable their use in this sector. Furthermore, the German Federal Government also planned to create certification procedures for smart contracts. As laid down in the Blockchain Strategy, the certification would be voluntary and would be carried out by an official body. Furthermore, the traceability of technology would be ensured by open-source solutions and the interoperability would be safeguarded by publicly documented standards and interfaces. According to an article from June 2021 (available at: https://www.heise.de/news/Blockchain-Strategie-der-Bundesregierung-lieferte-bislang-wenig-Ergebnisse-6114983.html) the majority of policy goals outlined in the 2019 Blockchain Strategy were still in a nascent phase.

During the research, national legal experts focused on horizontal challenges (including general contract law rules and consumer law) and also on certain sector-specific challenges. However, it should be noted that sector-specific challenges were reported on an ad hoc basis by national legal experts. In other words, no specific sector was subject to consistent scrutiny in this study. In the following paragraphs examples of horizontal and sectoral challenges are provided.

An example of a horizontal challenge, identified in Italy, concerns contracts that are more descriptive, or lack objectively measurable "if-then" conditions, as well as long-term contracts. These could be less suitable to codification as a smart legal contract. Whilst this challenge has been particularly noted in Italy, it should be borne in mind that such a challenge is not necessarily unique to Italy but could also exist in other EEA Member States.

Several examples of potential sectoral challenges exist for the use of smart contracts. Particularly, legal experts in fifteen EEA Member States **(AT, BG, DK, EE, ES, FI, HR, HU, IT, LI, LT, MT, NL, NO, PL)** indicated such potential challenges for the application of smarts legal contracts. The most common field of national law where challenges could potentially occur is property law **(**for example, in **AT**[49]**, BG**[50]**, EE**[51]**, ES**[52]**, FI**[53]**, HU**[54]**, LI**[55] **NL**[56]**, PL**[57]**),** where the sale of property (e.g., real estate) bears specific form obligations (e.g., written form; notarial certificate). Other areas of national law posing possible challenges include insurance law **(**for example in **EE**[58]**, HR**[59]**),** consumer contracts **(**for example, in **FI**[60]**, IS**[61]**, NO**[62]**),** loan contracts **(**for example, in **EE**[63]**),** gift contracts related to real estate **(**for example in **HU**[64]**),** the sale of a company **(**for example, in **AT**[65]**, LI**[66]**)** and the establishment of legal persons **(**for example, in **PL**[67]**).**

Lastly, another example for a sectoral challenge was found in **Malta**, which has legislation on smart contracts. In this legal system, innovative technology arrangement (ITA) certifications (issued by the Malta Digital Innovation Authority) for platforms using DLT or smart contracts can in certain cases be obligatory in regulated industries (financial services, gaming and communications). This could create obstacles for smart legal contracts. The reason is that ITA certifications are only provided by the competent Maltese authorities (the Malta Financial Services Authority, the Malta Gaming Authority or the Malta

[49] Article 431 of the Austrian Civil Code (ABGB), as well as Article 31 (1) of the Austrian Land Register Act (GBG).
[50] Article 18 and Article 26 of the Bulgarian Obligations and Contracts Act.
[51] Chapter 11 of the Law of Obligations Act of Estonia.
[52] Article 1280 of the Spanish Civil Code.
[53] Section 1 (Chapter 2) of the Finnish Code of Real Estate (540/1995).
[54] Article 6:215 (2) of the Hungarian Civil Code.
[55] Article 5 of the Land Transfer Act of Liechtenstein.
[56] Article 7:2 of the Dutch Civil Code
[57] Article 158 of the Polish Civil Code.
[58] Chapters 23-27 of the Law of Obligations Act of Estonia.
[59] Section 27 (Articles 921-989) of the Croatian Law on Obligations and Article 18 (2) on the Croatian Law on Insurance.
[60] Chapter 10 Section 6 of the Finnish Consumer Protection Act (38/1978, amendments up to 227/2011).
[61] Article 5(4) of Act No. 16/2016 on consumer contracts.
[62] Consumer Purchases Act.
[63] Chapters 21-22 of the Law of Obligations Act of Estonia.
[64] 6:235 (2) of the Hungarian Civil Code.
[65] Article 76 of the Austrian Limited Liability Corporation Act (GmbHG), as well as Article 62 of the Austrian Stock Corporation Act (AktG).
[66] Article 327 and Article 403 (4) of the Liechtenstein Personal and Corporate Law (PGR).
[67] Article 43 of the Polish Civil Code.

Communications Authority) if specific requirements for the use of smart contracts are met (e.g., appointment of a technical administrator).

3.2.2. Contract formation

Conclusion of a contract and its constitutive elements

A common requirement found across all EEA Member States for an offer to be valid is that it must include the essential elements set out in the national legislation. As a general rule in all EEA Member States, the principle of the *freedom of form* is established, according to which the parties are free to decide the form of the contract, unless there is a requirement of a specific form in the law.

The general rule on when a contract is considered to have been formed / created / concluded is when the offeror receives the acceptance of the offer. This rule is set out in this exact way in 19 EEA Member States (**BE**[68]**, BG**[69]**, CY**[70]**, CZ**[71]**, EE**[72]**, FR**[73]**, HU**[74]**, IE, IT**[75]**, LU**[76]**, LV**[77]**, PL**[78]**, PT**[79]**, SE**[80]**, SI**[81]**, SK**[82]). However, some variations exist among these EEA Member States. For instance, the offer's acceptance (which is the moment of the contract formation) can be done verbally or tacitly in **Bulgaria** and **Finland**. In ten EEA Member States **(CY, DE, EE, HU, IE, IT, LT, MT, NO, PL),** the contract is deemed formed also when the offer, which constitutes an act, is accepted (acceptance of the offer by conduct).

In some EEA Member States (for example, **DE, DK**)[83], a distinction between making an offer and an invitation to make an offer exists, which is particularly relevant in terms of e-commerce. An offer can be immediately accepted or rejected by the offeree, whereas an invitation to make an offer cannot simply be accepted by the offeree. Instead, it requires that the recipient of the invitation does not simply accept the offer, but does something additional. The recipient of an invitation to make an offer can, for example, approach on the basis of an advertisement and announce that he/she wishes to act on the basis of the advertisement. In other words, he makes the offer on the basis of the advertisement (solicitation), after which the advertiser can choose to accept the offer. This distinction is

[68] Civil code, article 5.21. In Belgium, the agreement of wills is not subject to any specific formalities and is formed by the sole agreement of the parties.
[69] Art. 14 of the the Act on Obligations and Contracts. Available at: https://lex.bg/laws/ldoc/2121934337.
[70] Section 10 of Cap.149 "Contract law". The principle of the absence of formalities in Cypriot contract law is established.
[71] Section 570(1) of Civil Code.
[72] Article 9 of Law of Obligations Act (*Võlaõigusseadus*), https://www.riigiteataja.ee/en/eli/ee/506112013011/consolide/current.
[73] Article 1101 et al. of the Civil Code.
[74] §6:5(2) of Civil Code.
[75] Art. 1326 of Civil Code.
[76] In Luxembourg, the agreement of wills is not subject to any specific formalities and is formed by the sole agreement of the parties.
[77] Articles 1470, 1533, 1536, 1537 of the Latvian Civil Law.
[78] Art. 70(1) Civil Code.
[79] The constitutive elements of a contract – offer, acceptance, intent – do not require any formalities other than the parties' consent in Portugal.
[80] Chapter 1 of the Contracts Act (*Lag (1915:218) om avtal och andra rättshandlingar på förmögenhetsrättens område*).
[81] Art. 21 of Obligations Code (*Obligacijski zakonik*, Official Gazette of the Republic of Slovenia, No. 97/07 with subsequent amendments).
[82] § 43c of Act No. 40/1964 Coll. Civil Code.
[83] Similar customary or legislative rules may be existing in other Member States too.

crucial when determining the legal position of the parties: a seller would be bound by an offer but can reject the buyer's offer made on the basis of an invitation to make offers.[84]

Another general condition applicable across the EEA Member States is that the acceptance of the offer must mirror the offer. In other words, the offeree has to accept the offer without changes. If the offeree accepts the offer with reservations or makes any changes, it is considered to be a new offer (counteroffer). However, in **Hungary**, the Civil Code does not require the acceptance be the mirror image of the offer. Rather, if the acceptance contains additional and/or different terms that qualify or alter the essential terms of the contract but does not amount to a counteroffer, the contract will be formed with such acceptance, and thus, the terms proposed will become part of the contract unless the offer expressly limits such possibility or the offeror objects without delay.

In case of smart legal contracts, different acts could be considered as constituting an offer from a contract law perspective, depending on the specific circumstances at stake. For example, where a smart contract is used to merely implement a written contract, the offer can occur in spoken or written word off-chain. Where the smart legal contract itself serves as a smart legal contract, the posting of the on-chain smart contract on the distributed ledger can be considered to constitute the offer.[85] The abovementioned national provisions on the acceptance of the offer can occur either by performance or by the authorization of a transfer, i.e., by signature or by means of a personal cryptographic key, that indicates that existing rules on offer and acceptance should not pose fundamental challenges for the formation of smart contracts.

Nonetheless, challenges can arise in relation to the constitutive elements of a contract. Particularly, as mentioned in the **Maltese**, as well as the **Romanian** and **Cypriot** national reports, a challenge with 'lawful consideration' (causa) and/or its moral character may arise. As per the Maltese Civil Code, the consideration is unlawful if prohibited by law or contrary to morality or to public policy. In cases of smart legal contracts used for illegal purposes where the contract is not enforceable, a challenge arises in view of the fact that the smart contract is embedded and automated. It should be noted that in **Malta** the courts make use of the theory of information, whereby a contract is deemed to be concluded where there is knowledge of acceptance by the party who made the offer. The use of this theory in relation to distance contracts may not be the most appropriate for smart contracts. With time stamps clearly determining the exact moment of acceptance and thus conclusion of the contract, smart contracts apply more the theory of declaration which holds that the contract is concluded as soon as there is manifestation of consent, even if the person who made the offer is not aware that his offer has been accepted.

National laws contain varying rules related to the declaration of intent. In **Bulgaria**, for instance, declarations of intent and promises are, in general, not equivalent to an

[84] However, it should be noted that for certain types of offers certain rules of presumption have developed in the literature and jurisprudence in relation to the distinction between offers and invitations to make offers. Particularly:

- Price marking (e.g., in a store) is generally regarded as an offer that the customer can accept by taking the item off the shelf and going to the checkout and paying. The retailer will thus be obliged to sell the product to the customer at the stated price. This, of course, on the condition that the product is not labelled at an incorrect price due to an obvious error;
- Advertising in print and in the media (e.g., in offer catalogs and newspapers, TV advertisements, etc.) are generally not regarded as actual offers, but rather as an invitation to make an offer;
- Advertising on the internet is generally regarded as an offer, as internet advertising does not have the same protection considerations in relation to the advertiser as with print and media advertising, as the latter has the option to remove the advertisement without further notice when the item is sold out.

[85] It should be noted that this is a general observation and holds true not only for Hungary but, potentially, for any Member State.

acceptance of an offer and, as such, are not deemed part of the constitutive elements of a contract. In **Estonia,** on the other hand, the contract is deemed concluded also by the mutual exchange of declarations of intent in any other manner if it is sufficiently clear that the parties have reached an agreement. Furthermore, in **Cyprus**, intent is defined as the union of a proposal/offer and an acceptance, thus constituting an essential element. In **Denmark,** the acceptance of an offer is considered to be a binding declaration of intent that contains both a promise and an injunction.

Germany gives particular weight to the declarations of intent: according to the German Civil Code, a valid contract comes to existence when there are valid declarations of intent by at least two persons (offer and acceptance).[86] The declaration of intent becomes effective upon receipt by the other party (i.e., when the offer reaches the offeree and acceptance reaches the offeror). A declaration of intent is deemed to have been received if the declaration has entered the recipient's sphere of influence in such a way that it is to be expected that the recipient will take note of it under normal circumstances. In other words, actual knowledge of the declaration by the recipient is not required. In relation to declarations of intent, it should be noted that the revocation of the offer or acceptance can be considered only if it arrives before or at the same time as the declaration of intent. Since "declarations of intent" through smart contracts would arrive very quickly, such revocation may be ruled out in most cases.

Similarly, two other EEA Member States' laws stipulate that a contract is deemed concluded at the time when the offeror receives a declaration of its acceptance from the offeree (**PL, SI**).

In **the Netherlands,** the conclusion of a contract is related to the declaration of intent ('a will directed to legal effect', as per the Dutch Civil Code) of both parties (as mutually understood by the other) by means of statements and conduct that is reasonable. Even if the will does not correspond to the declaration, the declarant is still bound by the declaration, if the other party could trust that the declaration did correspond to the will. This principle of justified reliance prevents an overly one-sided emphasis on the party's will. However, as can be seen in the law, the promise or will as the basis for binding contracts does not provide a sharp criterion for distinguishing between legally enforceable obligations and other promises that are not and where non-fulfilment leads at most to moral disapproval. Whether an agreement is binding or not depends on the circumstances of the case and the views of the trade.

[86] The contents of these declarations of intent must correspond and be made with reference to each other.

It was noted by the national experts with regard to nine EEA Member States (**AT**[87]**, DK**[88]**, FI**[89]**, HR**[90]**, IS**[91]**, LI**[92]**, LT**[93]**, NO**[94]**, RO**[95]) that a contract is deemed concluded once the parties' consent is given. Similarly, in **Spain**, contracts enter into force as soon as one or more persons agree to be bound, with respect to another or others, to give something or provide a service and bind the parties by mere consent. Nonetheless, according to the Spanish law, the following requirements need to be met to consider that a contract has been formed / created / concluded: (a) consent of the contracting parties, (b) true object that is the subject of the contract; and (c) established cause of the obligation. Regarding the consent of the contracting parties**,** according to the Spanish Civil Code, "in contracts concluded through automatic devices, there is consent from the moment the acceptance is manifested". This acceptance in a smart legal contract does not have any complications since it can be manifested in various ways, including via an electronic signature.

It should be noted that the **Greek** legislation contains a specific provision on the conclusion of smart contracts. Particularly, a smart contract is deemed formed / created / concluded as soon as the declaration of acceptance of the proposal from the other party reaches the offeror.[96] The acceptance is deemed to have occurred through the DLT when the acceptance is selected and published by the parties on the ledger technology.

Electronic contracts and contracts concluded through electronic communication

Some EEA Member States also have specific rules regarding contracts concluded in electronic form. In **Hungary**, electronic contracts become effective when they become accessible to the other party, regardless of when that party actually accessed the information. For contracts concluded using electronic communication to be considered valid and in force, three conditions on the form/medium in which the statement is expressed must be satisfied cumulatively:

- It must allow for the retrieval of unaltered content of the statement,
- It must enable the identification of the person who provided the statement, and
- It must enable the precise identification of the time when the statement was made.

In **Malta**, an electronic contract (particularly one for provision of services) is concluded when, after placing an order, the recipient of the service has received from the other party an acknowledgement of receipt of the order made by the recipient, provided that they acknowledge the receipt of the order made by the recipient without any undue delay and by electronic means. The order and the acknowledgement of receipt are deemed to have been received when the parties to whom they are addressed are able to access them.

[87] This process does not require any formalities in Belgium.
[88] The constitutive elements of a contract – offer, acceptance, intent – do not require any formalities other than the parties' consent in Denmark.
[89] No further formalities are required in Finland.
[90] The legal theory defines that a contract is concluded at the moment of acceptance of the offer. The Law on Obligations prescribes the same moment in Article 247, which says that the contract is concluded when the contracting parties have agreed on the essential ingredients of the contract.
[91] The constitutive elements of a contract do not require any formalities other than the parties' express consent.
[92] This process does not require any formalities in Luxembourg.
[93] Article 6.162(2) of the Civil Code is a complementary provision to paragraph 1, which provides that it is sufficient for the formation and validity of a contract that the parties agree on its essential terms.
[94] In the Norwegian system the contract is formed when an offer and its acceptance are concurrent and when the parties consent as to its vital elements ref. Norwegian Contracts Act (Avtaleloven, 1918), Lov om avslutning av avtaler, om fuldmagt og om ugyldige viljeserklæringer [avtaleloven] - Lovdata.
[95] In general, there are no particular formalities that the parties' consent must meet in order for a contract to be considered validly concluded.
[96] In accordance with article 192 of the Civil Code.

It was noted in the **Polish** national report that an offer submitted in electronic form is binding on the applicant if the other party immediately confirms its receipt.[97] The electronic form is considered valid if a declaration of will is submitted in electronic form and affixed with a qualified electronic signature (QES).[98]

In **Sweden**, the form requirement of concluding an agreement in writing is generally considered to be fulfilled electronically if the legislation does not specifically prohibit it. Such cases are rare in Sweden, as the principle of freedom of contract is implemented rather broadly in the country's legal system. In this case, an electronic signature in the form of an advanced electronic signature (AES) fulfils the necessary requirements, as per Articles 3 and 25 of the eIDAS Regulation.

Place of the conclusion of the contract

The place of the formation/conclusion of the contract varies across EEA Member States. Some examples on the place of the conclusion of the contract are as follows:

- Where the offer is made (**BG**),
- If the offer and acceptance are made at the same place, that is the place of the contract conclusion; otherwise, the place will be the seat of the party making the offer or the place of domicile or in the absence of this the habitual residence of the natural person (**HU**),
- Where the last act necessary to make the contract binding occurs, and where the offeree's performance starts, in case of acceptance by conduct (**IT**),
- The place of receipt of the declaration of acceptance by the person submitting the offer (**BE, PL**),
- The place of residence or the headquarter of the person submitting the offer at the time of concluding the contract in electronic form (**PL**).
- For a contract concluded by electronic means, the place is presumed to be the domicile of the offeror, unless the parties agree otherwise (**BE, LU**),
- The place where the offeror had their head office or place of residence at the moment the offer was made (**SI**).

Challenges

As noted above, the principle of the *freedom of form* is in place, unless there is a requirement of a specific form in the law. Such specific forms mostly relate to the need to register a contract or its object with public authorities, or to the requirement of a notarial deed for the conclusion of the contract.[99] At the time of writing, this can constitute a challenge for smart contracts,[100] as it is not possible to conclude a smart legal contract by means of a public deed, as such formalities cannot be satisfied by smart legal contracts. Form requirements are discussed in more detail in section 3.2.3.

[97] It should be noted that this can hold true for other EEA Member States as well.

[98] QES as defined in Articles 3 and 25 of the eIDAS Regulation.

[99] For instance, notarial authentication, along with public registration, is required for contracts on immoveable property in 17 Member States. In three Member States, notarial authentication is required also for contracts on some types of moveable property. This aspect is further discussed under section 3.1.3 on form requirements.

[100] The blockchain technology could, nonetheless, be useful for notaries, and its introduction into the notarial services, if possible, could facilitate both their work and the use of smart contracts for contracts which require a specific notarial authentication for their validity.

Regarding the abovementioned discussion, it should be noted that some uncertainties continue to exist as to the validity of smart legal contracts. For instance, as discussed in the **Estonian** national report, one challenge is that the offeror may not become aware of the acceptance at the same instance the pre-requisites for the execution of the smart contract are fulfilled. The **French** and **Romanian** national reports found that the consent of the parties and its validity or integrity may be difficult to fulfil in smart legal contracts, as the developers are the only ones capable of coding the conditions of the contract. Although these challenges related to the validity were noted in specific national reports, they may also be applicable in other EEA Member States.

In **Germany,** the main potential challenge is that it is not clear whether a valid declaration of intent can be attributed to a human when smart legal contracts are used, as currently German law does not recognise computers/machines as legal entities, hence they cannot declare intent.[101] In other words, in absence of legal personality for computers, the use of smart legal contracts in Germany is questionable, as no valid declaration of intent is possible. While this has been particularly noted in the German national report and literature, it should be borne in mind that such a challenge is not necessarily unique to Germany but could also exist in other EEA Member States.

In **Spain**, compliance with the consent requirements, given the “anonymity” of permissionless blockchain and the fact that most of the smart contracts will be signed remotely and without the parties knowing each other can generate some conflict in smart legal contracts. However, it should be noted that in their agreement to use smart contracts, the parties can provide for accepted levels of disclosure, thereby overcoming the issue of anonymity. In this case, before signing a contract, it should be checked if the consent is vitiated or if the parties have the legal capacity to sign a contract (minor, incapable, lack of representation etc.).[102] Otherwise, the contract could be null or void. Consent can only be granted by people and supposes the externalization of an internal will.

Validity requirements and differences between B2B and B2C contracts

Generally, the main legal requirements that can be difficult to fulfil with smart contracts are the information requirements in B2C contracts, as well as form requirements. These aspects are discussed in sections 3.2.2 and 3.2.5. The main validity requirements, while having similarities, vary across the EEA Member States. The following validity requirements have been identified in the national legislation of selected EEA Member States, examples of which are presented below:

- Must not offend common decency or violate legal provisions (**AT, LI**),[103]
- To include offer and acceptance of offer (**BG, CZ, DK**),

[101] While this was noted particularly in the German national report, this is potentially the case also in other Member States. It should also be noted that this refers to the scenarios when the actions of machines cannot be attributed to a person that has legal personality due to the anonymisation of transactions.

[102] It should be noted that the legal capacity has been identified as a validity requirement also in several other EEA Member States, as noted in the next subsection.

[103] While this requirement was explicitly mentioned in the national reports for Austria and Liechtenstein, it could be existing in other EEA Member States as well.

- A specified or determinable, as well as lawful object and content of the contract (**BE, BG, CY, DE**[104]**, ES, FR, HU**[105]**, IE, IT, LU, LV, NL**[106]**, RO, SE, SI**),
- Follow the specific form when required by law (**BG, DE, LV**),[107]
- Legal capacity of the parties to contract (**BE, CY, DE, ES, FR, HU, LU, RO, SI**),[108]
- Contain an intention to be bound (**CY, CZ, IE, IT, LV, SK**),
- Contain a consideration (**CY**[109]**, IE**[110]),
- Valid and clear declarations of intent (**DE**[111]**, FI**[112]**, HU**[113]**, SI**[114]),
- Not constitute initial objective impossibility (**SI**),
- The contract having been concluded in good faith (**DE**),
- Free and informed consent of the parties, without threat, error, trickery or duress (**AT**[115]**, BE, CY, FR, IS**[116]**, LI**[117]**, LU, LV**),[118]
- Agreement on the essential elements of the contract (**CZ, HR, HU, LT, LV, NO**),[119]
- Non-usurious price (**HU**),
- Be directed towards a particular (i.e. identifiable) party (**SE**)[120].

In **Austria** and **Liechtenstein**, in addition to the abovementioned requirements, special rules apply for standard terms and conditions, which are highly likely to also apply for smart contracts due to their standardised character. Clauses in terms and conditions or other standardised forms must not cause a significant disproportion of contractual rights and obligations if the other party to the contract did not have to expect them also according to the circumstances, especially according to their external appearance and was not explicitly referred to the clause.[121] This may affect B2C, as well as B2B contacts, although specific rules (for example, rules on unfair contract terms) apply to B2C contracts only. It should be noted that similar rules are likely to be found also in the national laws of other EEA Member States.

[104] The subject matter and content of the contract must be contained in the offer in such a definite or determinable manner that acceptance can be effected by a simple "yes". The offer must therefore contain all essential points of the intended contract (*essentialia negotii*).
[105] The subject matter of the contract must be possible, legally allowed and compliant with good morals.
[106] The requirement of any contractual obligations assumed by the parties to be sufficiently determinable is fulfilled if the determination of the obligations can be made according to predetermined criteria.
[107] While this requirement was explicitly mentioned in the Bulgarian, German and Latvian national reports, it could be existing in other EEA Member States as well.
[108] This list is not exhaustive, as it can be safely assumed that the possession of a legal capacity to sign a contract is crucial in any legal framework. The EEA Member States noted in this list contain particular provisions on legal capacity as a validity requirement.
[109] Consideration means that both parties must have an interest in the contract, which means that, for instance, promise of gifts are not valid contracts. Nevertheless, in Cyprus, a specific exemption is added in section 25 (2) of cap.149, which states that "nothing in this section shall affect the validity, as between the donor and done, of any gift actually made". Put differently, if the gift is already executed, it becomes a valid contract even if no consideration exists. Practically, because of the self-executing nature of the smart contract, consideration's issue will be solved.
[110] Unlike Cyprus discussed above, in Ireland there is a rule against past consideration, according to which "a promise given in return for a consideration which has already been supplied […] is not a contractual promise and cannot be enforced."
[111] There should be no mistake in intent, the intent should be freely expressed (no coercion/duress) and there should be no deceit.
[112] To be valid, the clarity of the parties' expressions of intention must be possible to be demonstrated.
[113] If there are any problems with the will that was expressed (mistake, duress, and undue influence) that will affect the validity of the contract and remedies will be available for the injured party.
[114] The manifestation of the intention to conclude the contract must be free and genuine (without threat, mistake, or deceit).
[115] None of the parties must be involved in the contract by threat, error or trickery.
[116] The only requirement for the validity of the contract is an approval by the recipient's free will, i.e. by self-determination and without the interference of others.
[117] None of the parties must be involved in the contract by threat, error or trickery.
[118] This list of the Member States is not exhaustive and this requirement may exist also in other Member States.
[119] Ibid.
[120] Section 1(1) of Contracts Act. This requirement may exist also in other Member States.
[121] Section 864a of the Civil Codes of both Member States (Allgemeines bürgerliches Gesetzbuch, AGBG).

The **Norwegian** legislation stipulates that, where digital services are provided in a B2C setting, the agreements that are based on standard terms must not be "unreasonable".[122] To assess the reasonable nature of the terms, the balance between the parties' rights and obligations is to be taken into account, as well as the clarity of the contract.

Notably, in **Estonia**, the validity of a contract is not affected by the fact that when the contract was entered into, the performance was impossible. This can be relevant for smart contracts in the sense that they would not lose their validity, even if the performance of the contract's subject was not possible when the contract was concluded. Furthermore, even if one of the parties did not have the right to dispose of a thing or right which is the object of the contract, this does not affect the validity of a contract. Although this was noted in the Estonian national report, this can hold true also for other Member States (e.g., such a rule exists in Austria and Germany).

In **Greece**, the national legislation stipulates that a smart legal contract binds the parties upon the completion of their accession to it.[123] If in electronic transactions the electronic signature constitutes a valid way to be bound by the contract, smart legal contracts, which are compiled by electronic means and signed by a cryptographic key, can also be considered valid for binding the parties. Nonetheless, it should be borne in mind that, according to Article 8(1) of Presidential Decree 131/ 2003,[124] although electronic signatures may be concluded by electronic means, this provision does not apply "(a) to contracts which establish or transfer rights in rem in immovable property, (b) to contracts requiring the law to resort to courts, public authorities or professions exercising public authority, (c) in contracts falling within family or family law."

In terms of the intent to be bound, **Italian** legislation contains some mandatory rules that aim to guarantee that the contracting party had the intent to be bound by the contract in question and is aware of its content, especially for consumers (as a weaker party). In particular, according to Article 1341 of the Italian Civil Code on standard contracts, the terms of the contract are effective only if the party who accepts them had a sufficient chance to know their content, which means that for some kinds of clauses (e.g., limitation of liability, contract withdrawal etc.) there is a need for separate and specific approval in writing, i.e. a hybrid smart contract.

A detailed list of requirements for a contract to fulfil exists in **Poland** (Article 66 and following Articles of the relevant section of the Civil Code)**.** These, particularly, include:

- Specification of the type of contract.
- Designation of the date and place of the contract.
- Designation of the parties to the contract.
- Identification of the parties' statements (expressions of will).
- Indication of the duration of the contract.
- Determining how to terminate the contract.

[122] Marketing Control Act (markedsføringsloven), § 22. This derives from Directive 93/13 on unfair terms in consumer contracts and holds true for all Member States.

[123] Article 49(1) of Law 4961/2022.

[124] Presidential Decree 131/2003 available at [https://www.taxheaven.gr/law/%CE%A0.%CE%94.131/2003] , last accessed 22/10/2022.

- Determining the liability of the parties to the contract.[125]
- Indication of legal provisions.
- Definition of the final provisions of the contract.

In terms of legal uncertainty surrounding smart legal contracts, one area relates to mistakes,[126] as the validity of a contract can be questioned where incorrect information has been given. For instance, as pointed out in the **Swedish** national report, where mistakes exist in the code of a smart contract, it is unclear under which circumstances the contracting parties should have known of the mistake, and as a result whether or not the mistaken information would be binding. In this regard, the abovementioned **Estonian** legislation may prevent such challenges in relation to smart contracts.[127] In **Slovenia**, in cases of misunderstandings, a party may rely on a mistake only if it relates to essential features of the subject matter, person or circumstances and is excusable, i.e. that it occurred despite the party's exercise of due care. Other challenges related to smart legal contracts concern the consent of the parties and possible defects in it, as well as the challenges in establishing the legal capacity.

An additional challenge for the validity of the contract may arise in relation to the requirement of legal capacity. As pointed out in the **Cypriot** (as well as **Italian** national reports), it is not always possible to verify the identity of the parties of the contract and, consequently, whether they have the legal capacity for the contract, which can cause an uncertainty in terms of the validity of the contract.

Due to the regulation of consumer rights in place at the EU level, some differences exist between B2B and B2C contracts (e.g., the right of withdrawal within 14 days, information requirements etc). In one Member State (**MT**) particularly some requirements differ depending on the B2B/B2C nature of the contract. In **Malta**, as noted earlier, an electronic contract is concluded when, after placing his order, the recipient of the service has received from the service provider an acknowledgement of receipt of the order made by the recipient. In this regard, the law allows for derogations in the case of a B2B but not B2C relationships.

Finally, some general conclusions can be drawn about the differences between B2B and B2C contracts. While the principle of *freedom of form* applies to all contracts (unless stipulated otherwise in law) and would thus include code-only smart contracts by analogy, in practice the usage of smart legal contracts may be practically limited mainly to B2B contracts due to several reasons.[128] Firstly, businesses can have greater economic possibilities to consult experts and decipher the code should such an action be needed, which can further strengthen their stance in comparison with the consumers. Moreover, it can be imagined that B2B smart contracts are concluded based on framework traditional agreements that set their main content and modalities of conclusion, which facilitates the

[125] It is noted in the Polish national report that this requirement may be a challenge for smart contracts, as “the allocation of responsibility for errors in the programme code may depend on how it was acquired,” and if it was acquired through open-source licence, the creator of the blockchain can avoid liability. Nonetheless, it should be noted that some mechanisms can be employed to avoid such a situation. It is suggested in the literature that this can be done by determining who uses the blockchain: “the method of fulfilling the task chosen by the entrepreneur (in this case, using a decentralised network) does not affect the mere existence of the obligation and the duty to fulfil it.” The entrepreneur’s obligation is based on Art. 474 of the Civil Code.

[126] However, it should be noted that a smart contract is expected to leave little room for mistakes in the form of wrong or misleading information, as this information is typically entered into the smart contract from outside. Moreover, parties can agree on oracles (trusted source of information), which can help to eliminate potential mistakes in this regard.

[127] This refers to the Estonian rule, according to which the validity of a contract is not affected by the fact that when the contract was entered into, the performance was impossible. Furthermore, even if one of the parties did not have the right to dispose of a thing or right which is the object of the contract, this does not affect the validity of a contract.

[128] Reported in the Estonian national report.

use of smart contracts in the B2B setting.[129] Finally, B2C contracts need to fulfil certain information requirements as per harmonised EU law, which can be a challenge for smart contracts. This is discussed in further details in section 3.2.5.

Validity of electronic contracts and electronic signatures

In connection with the validity of electronic contracts and signatures, Article 9(1) of the e-Commerce Directive[130] should be mentioned. According to this Article, the national legal systems shall allow contracts to be concluded by electronic means and shall in particular ensure that "the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means."

While thanks to the application of another EU-level legislation, the eIDAS Regulation the national laws are generally similar in requiring the use of a qualified electronic signature (QES) for an electronic contract to be deemed valid, the more specific rules on electronic contracts somewhat vary across the Member States and examples of such specific rules are presented below.

The **Austrian** law does not stipulate specific requirements for electronic contracts. However, if the type of contract requires a written form, Austria currently offers three types of QESs (mobile phone signature, card-based citizen card and ID Austria[131]) according to the eIDAS Regulation, with the same legal qualities as manual signatures (Para 4 sec 1 Signature Act (SignG)).

In **Belgium** and **Luxembourg,** any legal or regulatory requirement of form relating to the contractual process is deemed to be satisfied with respect to a contract by electronic means when the functional qualities of that requirement are preserved. The requirement of a written form is satisfied by a set of alphabetical signs or any other intelligible signs affixed to a medium which allows access to it for a period of time appropriate to the purposes for which the information is intended and which preserves its integrity, regardless of the medium and the means of transmission.

In **Bulgaria**, a contract can be electronic as long as the two main constitutive elements of the contract are present: declaration of will and consent.[132]

For an electronic contract to constitute a written contract in **Czechia**, the requirements of Sections 561 and 562 of Civil Code need to be complied with, i.e. it needs to:

i) capture the content of the legal action,
ii) acting person needs to be determined and
iii) the contract needs to be signed.

In **Estonia**, electronic contracts are not specifically mentioned but the legislation allows the existence of any form of contracts. If a contract has a written form and requires a signature

[129] Reported in the Italian national report.
[130] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').
[131] https://www.oesterreich.gv.at/themen/dokumente_und_recht/handy_signatur_und_kartenbasierte_buergerkarte/1/Seite.2821108.html.
[132] Articles 2, 3(2) of the Act on Electronic Documents and Electronic Authentication Services, available at: https://www.lex.bg/laws/ldoc/2135180800.

according to the Estonian legislation, then to form it as an electronic contract, a QES is needed.[133]

In **France**, for an electronic signature to have evidential value, it must benefit from a presumption of reliability, which results from the use of an identification process established through a secure electronic signature creation device and allowing the verification of this signature by using an electronic certificate issued by a qualified provider.[134] More precisely, for an electronic signature to be deemed reliable, it must meet the following conditions:

- It must be uniquely linked to the signatory;
- It must make it possible to identify the signatory;
- It must be created by means that the signatory keeps under his exclusive control; and
- There must be a link between the signature and the act to which it is attached. These conditions seem to be fulfilled in the blockchain.

However, the French legislation also requires that the electronic signature is verified by means of a certificate issued by a qualified and approved service provider. In this regard, a decision of the Court of Cassation, dated 6 April 2016,[135] enabled new perspectives. The case involved a person who denied that he was the author of an online application for supplementary insurance and refused to pay the premium on the grounds that the online contracting platform did not use a qualified electronic certificate. The Court of Cassation ruled against him, having found that the judge had sufficiently verified the intrinsic conditions of reliability of the said signature. This means that there is no longer a need to provide a certificate. As a result of this ruling, the blockchain would be deemed to offer the guarantee of an electronic signature within the meaning of the law.

In **Germany,** the general rule that contracts do not need to fulfil a certain form requirement unless otherwise prescribed in law applies. Nonetheless, if a contract is concluded in an electronic form, each party must sign with an electronic signature (which can be a simple e-signature in most cases). However, if the contract requires a written form by law, then only a qualified electronic signature can be used in accordance with the Trust Services Act[136] for such a contract in electronic form.[137] Furthermore, there may be cases where the law explicitly prohibits replacing the written form of a contract with an electronic form (for example, for the declaration of suretyship).[138] Where an official certification or notarial recording is required, this cannot be fulfilled simply with e-signature.

According to the **Greek** legislation, where a signature or seal is required for the conclusion of a smart contract, it may be placed in the form of an electronic signature or an electronic seal.[139]

In **Hungary**, as mentioned earlier, electronic contracts become effective when they become accessible to the other party, regardless of when that party actually accessed the

[133] Article 11 (1), Law of Obligations Act (Võlaõigusseadus)/(LOA), available at: https://www.riigiteataja.ee/en/eli/ee/506112013011/consolide/current.
[134] https://graldinesalord.medium.com/les-smart-contracts-sont-ils-des-contrats-25f1bbd5e253.
[135] Cour de cassation, chambre civile 1, arrêt du 6 avril 2016.
Available at: https://www.legifrance.gouv.fr/juri/id/JURITEXT000032389405/.
[136] Vertrauensdienstegesetz (VDG), available at: http://www.gesetze-im-internet.de/vdg/BJNR274510017.html.
[137] Article 126a of the German Civil Code.
[138] Article 126 (3) of the German Civil Code.
[139] Article 50 of Law 4961/2022.

information. For electronic contracts to be considered valid and in force, three conditions on the form/medium in which the statement is expressed must be satisfied cumulatively:

- It must allow for the retrieval of the original, unaltered content of the statement;
- It must enable the identification of the person who provided the statement; and
- It must enable the precise identification of the time when the statement was made.[140]

In **Iceland**, Article 8(1) of Act No 30/2002 on Electronic Commerce and other Electronic Services states that where written contracts are required by law or administrative provisions, such contracts shall be replaceable by an electronic contract, provided that the contract is available to both parties and in preservable form.[141] According to the preparatory works (*travaux preparatoires*) of Act No. 30/2002, the condition of preservability means that it is possible to approach the content of the contract after it has been entered into. This condition can for example lead to the presentation of an electronic contract in court cases. When the law stipulates that the parties to the agreement keep their own copy, the condition is met when all parties to the agreement have access to it, even if it is in electronic form."

In **Ireland**, there are a small number of **legal documents that may not be executed by electronic signature**, including wills and interests in real property. More specifically, the Electronic Commerce Act 2000 stipulates the excluded laws in section 10 (namely, a will, codicil or any other testamentary instrument to which the Succession Act, 1965 applies; a trust; or an enduring power of attorney). However, these exclusions are accompanied by specific provisions that allow the Minister to extend the application of the Act or a provision of the Act to these excluded laws if they are of the opinion that '(a) technology has advanced to such an extent, and access to it is so widely available, or (b) adequate procedures and practices have developed in public registration or other services, so as to warrant such action, or (c) the public interest so requires'.

As per the **Italian** legislation, electronic contracts are considered valid under the same conditions of validity as traditional contracts. An electronic document is deemed to be in written form when the signatory signs it by using a digital signature, a qualified electronic signature, or an advanced electronic signature.[142] Qualified and advanced electronic signatures are disciplined by the e-IDAS Regulation, while the digital signature is peculiar to the Italian legal system and consists of a qualified electronic signature that makes use of asymmetric cryptography. In addition, the same legal value is recognised to a document formed under the requirements set by the Agency for Digital Italy (AGID) pursuant to Article 71 of the CAD, prior to the IT identification of its author, in such a way as to guarantee its security, integrity, and immutability and the fact that it is ascribable to the author, clearly and unequivocally. In all other cases, the suitability of the document to satisfy the requirement of the written form can be freely assessed in court, with respect to its characteristics of security, integrity, and immutability.

The **Liechtenstein** law does not stipulate specific requirements for electronic contracts. However, if the type of contract requires a written form, in Liechtenstein the "qualified trust service providers", such as DocuSign or Skribble, offer ways to electronically sign documents with the same legal qualities as manual signatures (Art 3 sec 1 Signature and Trust Service Act (SigVG)).

[140] Mihalics Law Firm, *Az elektronikus szerződéskötésről* [About electronic contracts] 2021.11.29, available at https://mihalics.hu/az-elektronikus-szerzodeskotesrol/.

[141] The Act on Electronic Commerce and other Electronic Services can be found here: https://www.althingi.is/lagas/nuna/2002030.html

[142] Article 20(1-bis) of the Code of Digital Administration (CAD).

In **Malta**, electronic contracts are legally valid and are deemed to be formed (unless otherwise agreed by parties that are not consumers) when, after the placement of an order, the recipient of the service has received an acknowledgement of receipt from the service provider.[143] In terms of signature, it is only with QES under the eIDAS Regulation that legally binding status can be guaranteed. It should be noted that while most blockchains meet the criteria laid out for Advanced Electronic Signatures (AES), it is not the same with QES. The author of a QES will need the approval from a Certificate Authority with the issuance of a digital certificate. This is a costly and time-consuming process to achieve and although technically possible for a smart contract to be signed by a QES, it may defeat the purpose of a permissionless decentralised ledger.

The **Dutch** legislation accepts an electronic record on a durable medium, with or without an electronic signature.[144] The main aspect that may be a challenge for smart contracts in this regard is that the requirement of viewability might involve sharing the source code, which could be a problem.[145]

With regard to electronic contracts, the **Polish** legislation stipulates that an offer submitted in electronic form is binding on the applicant if the other party immediately confirms its receipt.[146] Moreover, if a trader is submitting an offer in electronic form, it is obliged to inform the other party in an unambiguous and understandable manner before concluding the contract about certain aspects of the contract.[147]

In **Portugal**, declarations issued electronically meet the legal requirement in writing when contained in a support – namely a digital one - that offers the same guarantees of reliability, intelligibility and conservation.[148] Furthermore, the electronic document is valid as a signed document when it meets the requirements of the legislation on electronic signature and certification (QES).[149]

In **Romania**, a written signature is not necessarily required for a valid contract, as contracts are generally valid if legally competent persons reach an agreement, whether they agree verbally, electronically or in a physical paper document.[150] To prove the existence of a valid contract, parties sometimes have to present evidence in court. Leading digital transaction management solutions can provide electronic records that are admissible in evidence under Romanian laws.[151] Moreover, an electronic document which incorporates or to which an extended electronic signature, based on an unsuspended and unrevoked, at that particular time, qualified certificate and generated with a secured device for the issuance

[143] Article 10 of the Electronic Commerce Act.
[144] Article 6:227a BW/Dutch Civil Code.
[145] https://www.bjutijdschriften.nl/tijdschrift/contracteren/2018/2/Contr_1566-0893_2018_020_002_004?session_key=b8d5bb90-2398-013b-78b9-00505686425b.
[146] Art. 66^1 of the Polish Civil Code, Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, Dz.U. 2011 Nr 199 poz. 1175, ostatnio zmieniana 2022, Act of 19 August 2011 on payment services, Journal of Laws No. 2011 No 199, item. 1175, last amended 2022, available at https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20111991175..
[147] Particularly, this includes the following:
1) technical activities that make up the contract conclusion procedure;
2) legal consequences of confirmation by the other party of receipt of the offer;
3) the rules and methods of recording, securing and sharing by the entrepreneur to the other party the content of the concluded contract;
4) methods and technical measures for detecting and correcting errors in the data entered, which they are obliged to make available to the other party;
5) languages in which the contract may be concluded;
6) codes of ethics that apply, and their availability in electronic form.
[148] Article 26 number 1 of the Decree No. 7/2004.
[149] Article 26 number 2 of the Decree No. 7/2004.
[150] Article 1166 of the Romanian Civil Code.
[151] Under Articles 266, 267, corroborated with Articles 283, 284 or 310 of the Romanian Civil Procedure Code.

of an electronic signature, was attached or was logically associated, is assimilated, in what concerns its conditions and effects to a handwritten signed document.[152] An electronic contract is deemed written if:

- it is signed with a valid qualified electronic signature (QES) by a signatory or its legal representative (for legal entities);
- the time of the signature can be identified; and
- the content of the electronic document is unchanged and this can be proved (integrity).

According to the **Slovenian** legislation, a service provider that concludes contracts by electronic means shall ensure contractual terms and general conditions in such a form that allows the service recipient to store and reproduce them**.**[153]

In **Spain,** electronic contracts will be considered valid and effective, when the consent and other requirements necessary for its validity concur. Moreover, for the conclusion of contracts electronically to be valid, the prior agreement of the parties on the use of electronic means will not be necessary.[154]

In **Sweden**, electronic contracts follow the same rules as other types of contracts, due to the general lack of rules on form requirements within Swedish law. A contract, electronic or smart, will therefore be valid provided the general contractual rules have been followed.

It is safe to assume that the abovementioned requirements on electronic contracts in the EEA Member States would be applicable to smart legal contracts. However, it is not free of potential challenges for smart contracts, albeit not impossible to overcome. Such challenges are, inter alia, ensuring the authenticity and integrity of parties' consent, the fulfilment of the requirements on electronic signature by smart contracts, the fulfilment of the requirement on the use of a durable medium for the conclusion of an electronic contract, the stipulating of contractual terms and general conditions in such a form that allows their storage and reproduction.

Thus, the main challenges in terms of the application of the provisions of electronic contracts to smart contracts are more general in nature and are not necessarily a challenge because of the rules on electronic contracts specifically. Rather, such challenges can occur also if smart contracts are covered by other types of contracts.

Identification and number of parties in a contract

In most EEA Member States there are no specific requirements in terms of the number of parties in a contract, which may indicate that a contract can involve one or more parties. In one EEA Member State (**NL**) a requirement is set out explicitly requiring that one or more parties be involved in a contract.[155]

It should be noted at the outset that requirements of identification exist in all EEA Member States in relation to consumer contracts. Moreover, exceptions from any lack of

[152] Article 5 of Law no. 455/2001.

[153] Art. 7 Electronic Commerce Market Act, *Zakon o elektronskem poslovanju na trgu* (Official gazette of the republic of Slovenia, No. 96/09 with subsequent amendments, "ZEPT").

[154] Law 34/2002 on Services of the Information Society and Electronic Commerce, 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.

[155] Article 6:213 paragraph 1 BW/the Dutch Civil Code.

requirements in terms of identification of the parties apply in relation to Directive 2015/849 in all EEA Member States,[156] as according to Article 13(1)(b), EEA Member States shall establish customer due diligence measures which should comprise "identifying the beneficial owner and taking reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is." Finally, contracts which require notarial authentication or public registration imply the identification of parties.

Nonetheless, the situation varies for all other contract types. For instance, no requirement on specifying the identity is in place in the following EEA Member States (**AT, BE, BG, CY, DE, DK, EE, ES, GR, IE, IS, LI, LU, NL, PT, SE,**[157] **SI, SK**), while in one (**FR),** the person from whom the contract emanates should be duly identified. In the following EEA Member States (**HU**[158]**, IT**[159]**, MT**[160]**, PT**[161]), depending on the type of the contract or on the sector, identification requirements exist. In some EEA Member States (**CZ, FI, HR, LT, LV, NO, PL, RO**), the parties need to be identified in order to conclude a contract by a document.

Verification by an auditor or a trusted third party (TTP)

An obligatory verification is not foreseen in the majority of EEA Member States, with the exception of **Malta**. Nonetheless, as smart legal contracts need to be electronically signed, there is the need to obtain a certified signature issued by a certifying entity in Malta. In addition, in **Croatia** as per Article 41 of the Law on electronic communications,[162] "operators of public electronic communication networks and services and networks used to support critical infrastructure systems must take appropriate technical and organizational measures to protect the security of their networks and services. The measures taken must ensure a level of security that corresponds to the existing level of danger for the security of the network and services, taking into account the available technical and technological solutions. In particular, measures which include coding (encryption) when appropriate, which prevent and reduce the impact of security incidents on users and on other electronic communication networks and services should be undertaken." Furthermore, the Law provides that an Ordinance shall prescribe the obligation to carry out an annual audit of network security measures and operator services, as well as the criteria and method of certification of legal entities authorized to carry out that audit.

[156] 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, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849.

[157] In Sweden, there is no requirement of identification. However, a number of national authorities are involved in the procedures surrounding electronic identification. These are:

- The Agency for Digital Government [Myndigheten för Digital Förvaltning (DIGG)] supports and coordinates the public sector in matters relating to secure electronic identification and is responsible for the Swedish eIDAS node Sweden Connect;
- The Swedish Post and Telecom Authority [Post- och Telestyrelsen (PTS)] is the main supervisory body and has the ability to issue regulations on requirements for creating qualified electronic signatures. It has issued (non-binding) guidelines on trusted services in Sweden [Vägledning för betrodda tjänster i Sverige enligt eIDAS];
- The Swedish Civil Contingencies Agency [Myndigheten för samhällsskydd och beredskap (MSB)] also plays a role, having the ability to issue regulations on security requirements linked to the creation of qualified electronic signatures.

[158] In Hungary, contracts for which a written form and signature is required, the parties must be identified.

[159] In Italy, when the law establishes that the contract has to be concluded in writing, identification of the parties is required in order to establish the capacity of the party to conclude contracts. In other situations, knowing the identity of the party is not mandatory but essential (for instance, for the ease of the litigation process).

[160] In regulated industries in Malta (financial services, gaming and communications), due to the anti-money laundering (AML) and know your customer (KYC) regulations, identification of the parties is required.

[161] In the case of real estate contracts, identity and capacity of parties should be revealed namely for tax reasons.

[162] https://www.zakon.hr/z/182/Zakon-o-elektroni%C4%8Dkim-komunikacijama.

In **Malta**, the application process for obtaining regulatory certification of innovative technology arrangements (ITAs) is established and is divided into two stages:

1. Gathering requisite documents and filing an application form to the Malta Digital Innovation Authority (MDIA). Once MDIA is satisfied with the general and specific requirements, it issues a Letter of Intent.
2. The System Auditor, appointed by the Applicant, evaluates the platform and is responsible for issuing an opinion on it. The opinion is later reviewed by the MDIA, and if the assessment proves positive the MDIA certifies the business in terms of the ITAS Act.

Hence, the applicant's software must undergo a thorough review by a registered System Auditor, which must be an independent third party. The System Administrator's task is to verify that the applicant's system meets pre-defined general and specific standards with reference to the purposes, qualities, features, attributes and behaviour of the ITA.

There are two types of System Audit:
Type 1: the System Auditor forms an opinion on whether a blockchain project is fairly explained and if the features within the project itself are fittingly crafted to meet the requirements. This is required for non-operative organisations (not yet alive or which have operated for up to 66 months).

Type 2: the Systems Audit covers the same points as defined in Type 1, but it also incorporates the auditor's opinion on the features efficiency throughout the period covered by the audit. Type 2 is mandatory following 6 months from the platform's launch date.

Choice of applicable law in cross-border transactions

No specific requirements (other than those set out either in Rome I Regulation[163] in terms of the choice of applicable law in cross-border transactions are established in 26 EEA Member States **(AT, BE, BG, CY, DE, DK, ES, FI, GR, HR, IE, IS, IT, LI, LT, LU, LV, MT, NO, NL, PL,**[164] **PT, RO, SE, SI, SK)**.

Some examples of specific provisions are set out below.

In **Czechia**, Act No 91/2012 Coll., on the International Private Law, applies, providing additional safeguards for consumers in B2C contracts. Section 87(2) of Act on the International Private Law stipulates that if a legal relationship established by a consumer contract is closely related to the territory of a Member State of the European Union, the consumer cannot be deprived of the protection under Czech law, if the proceedings take place in the Czech Republic, even if other law has been chosen for the contract or is otherwise to be used than of a member state of the European Union (mandatory provision).[165] This may pose a challenge in case of smart contracts which do not comply with this requirement. Section 87(3) of Act on the International Private Law stipulates that

[163] Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations, available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32008R0593.
[164] In Poland, if the applicable law is not indicated in the contract, or in the special provisions in force in Poland, or in ratified international agreements and EU law, the legal relationship should follow the law of the country with which the legal relationship (here: the smart contract) is most closely related.
[165] This is in line with Article 6(2) of Rome I Regulation.

insurance contracts[166] are governed by the law of the state in which the policyholder has his habitual residence. The contracting parties may choose the applicable law for the insurance contract; if it is an insurance contract to which a directly applicable regulation of the European Union applies, the contracting parties may, to the extent permitted by this regulation, choose any applicable law (mandatory provision). This may pose a challenge in case of smart legal contracts which do not comply with this requirement.

According to the **Estonian** legislation, in case the consumer is resident in Estonia or another EU Member State, and the contract was entered into as a result of a public offer, advertisement or other such activity in Estonia or the contract is essentially related to the territory of Estonia, the provisions on standard terms will apply.[167] This is the case even if the place of business, residence or seat of the party supplying the terms is not in Estonia. Furthermore, for contracts that contain standard terms related to the economic and professional activities of parties that have their places of business related to the contract or performance of the contract in Estonia, the provisions on standard terms will continue to apply, regardless of which state's law is applicable to the contract.[168] As smart legal contracts may rely on standard terms, the limitations to the choice of law clauses when dealing with consumers may be a challenge to be fulfilled.

In **France**, as a general rule, a close link with the territory of a Member State is to be taken into consideration. As per the French Civil Code, a close link with the territory of a Member State shall be deemed to be established in particular:

- If the contract was concluded in the Member State of the consumer's habitual residence
- If the trader directs his activity towards the territory of the Member State where the consumer resides, provided that the contract falls within the scope of that activity;
- If the contract was preceded in that Member State by a specific offer or advertising and by the acts performed by the consumer necessary for the conclusion of the contract;
- If the contract was concluded in a Member State to which the consumer went as a result of a proposal for a journey or holiday made, directly or indirectly, by the vendor to induce him to conclude the contract.

In **Hungary**, Act XXVIII of 2017 on International Private Law applies as a set of default rules for issues not falling under the scope of Rome I Regulation.[169] It does not directly address smart contracts or even electronic contracts and does not present a challenge for the use of smart contracts in cross-border transactions. In fact, the Act introduces the general rule that the parties have a free choice in the applicable law, their agreement to this effect is consensual and does not require any further formalities.

Challenges related to contract formation

Generally, in terms of contract formation, several common challenges were identified. One of these is related to the requirement of having a 'lawful consideration' (causa) in the contract and/or the moral character of the contract, which is challenging to verify due to the embedded and automated nature of smart contracts. In addition, since the validity of the contract can be under question in cases of the provision of incorrect information, there is

[166] Insurance contracts are excluded from the scope of Rome I Regulation, according to Article 1(2)(j).
[167] In line with Recital 25 of the Preamble of Rome I Regulation.
[168] In line with Recital 14 of the Preamble of Rome I Regulation.
[169] Exclusions from Rome I Regulation mentioned in its Article 1(2).

currently legal uncertainty about how potential mistakes could be handled. Moreover, the validity of the contracts can come under question if the requirements for the conclusion of the specific type of contract are not met. As discussed elsewhere in the text (e.g., Section 3.2.3), such requirements can represent a challenge for smart contracts. Finally, the legal capacity and consent of the parties can present challenges for smart contracts, as their validity is not always possible to verify.

The challenges to smart legal contracts in terms of the choice of applicable law in cross-border transactions lie in the global nature of public and permissionless blockchains, as these are generally not tied to a certain territory. Where a smart legal contract is deployed on such networks, it is difficult to determine the applicable law for claims arising in connection with a given contract. To overcome this challenge, clauses on the choice of law for dispute resolution in the smart legal contract could reduce this uncertainty and provide the necessary basis for a process of handling any disputes that may arise.

3.2.3. Form requirements

General or sector-specific form requirements for contracts

Various form requirements exist in the national legislation of most EEA Member States for specific contracts, the details of which are presented below.

Particularly, a notarial authentication (as well as a registration with the relevant public register) is required for contracts on immoveable property in 17 EEA Member States (**BE, BG, CY, CZ, DE, EE, FI, FR, GR, HU, LU, LV, MT, PL, PT, RO, SI)**. Such a requirement exists also for some types of moveable properties in several EEA Member States (e.g., **BG, CY, PT**). Some other EEA Member States require notarial authentication for usufruct agreements (e.g., **MT, PL**) and some EEA Member States stipulate such a requirement for matrimonial property agreements (i.e. **CZ, PL, SI**). Further types of contracts and their requirements (albeit non-exhaustive) are provided in the table below. The requirements of notarial authentication, registration with public authorities or of specific written form can constitute a challenge for smart contracts where they cannot be satisfied by smart legal contracts.

Table 2: Types of contracts with a notary-authenticated or written form requirement[170]

Form requirement	Type of contract	Member State
Authentication by notary required	Right in a legal entity	BG
	Charter of a foundation	CZ
	Donation	FR
	Marriage contract	DE
	Contracts for the establishment of partnerships	LT
	Agreement on establishing separate ownership of the premises	PL
	The creation of some companies, such as the joint-stock companies	PL
	Sale of inheritance	RO

[170] The types of contracts and the list of Member States provided in this table are indicative examples rather than an exhaustive list.

	Contracts relating to the disposition of the property of persons deprived of their legal capacity	SI
	Agreements on renunciation of an inheritance that has not been initiated	SI
	Contract of lifelong maintenance	SI
	Contract of subsistence	SI
	Contract on gift in event of death	SI
	Contract transferring the business of a sole proprietorship to other persons	SI
	Contract on the absorption, merger, or split-off of a company	SI
Written form required	Gift contracts if the gift is not handed over at the time of oral agreement	AT, LI
	A "bond in customary form" (a specific Cypriot contract that works as acknowledgment of debt)	CY
	In case of contracts implying interference with human integrity	CZ
	Contracts for the establishment of legal persons	CZ, LT
	Exhibition contract	CZ
	A pledge agreement, the subject of which is the pledge of a movable property that has not been handed over to the pledgee	CZ
	Settlement of the spouses' property relations[171]	CZ
	Agreement on the settlement of alimony for the period after divorce	CZ
	Credit agreement / consumer loan contract	DK[172], NO
	Consumer sureties	EE (QES required)
	Gratuitous contracts	EE (QES required)
	Timeshare contracts	EE (QES required)
	Life Annuity contracts	EE (QES required), LT
	Restraint of trade	EE (QES required)
	Gift commitment	DE
	Power of attorney	DE
	Contracts with public administration (public law contracts)	DE
	Bill of Lading (a transport document)[173]	FI

[171] Requires mandatory written form with officially verified signature. The official verification of signatures (so-called "legalisation") is governed by Act No 21/2006 Coll., on verification. A signature may be verified by regional authorities; municipal authorities; the Czech Post and the Chamber of Commerce of the Czech Republic. In addition, signatures may also be verified (under the respective legislation) by notaries, attorneys, captains of vessels, and consular and embassy offices of the Czech Republic abroad. The person needs to demonstrate his or her identity (i.e. by a citizen identification card or a passport) and declare that the signature on the document being verified is his or her.

[172] A credit agreement in Denmark must be drawn up on paper or on another durable medium. All contracting parties must have a copy of the credit agreement (Promulgation of the Act on Credit Agreements, LBK nr 817 of 06/08/2019, Article 8, section 1).

[173] Bill of Lading has to be signed in writing, mechanically or electronically, and distributed to both the shipper and the consignee in original.

	Contracts on immovable property	IS, SE[174]
	Contracts between natural persons where the amount of the contract at the time of conclusion exceeds one thousand five hundred euro, except for contracts which are executed at the time of conclusion	LT
	Hire purchase	LT
	Insurance	LT, NO
	Arbitration	LT
	Contracts for the lease of movable property for a period exceeding one year	LT
	Contracts for the sale of a motor vehicle	LT
	Contracts on movable property	MT
	Consumer bail towards financial institutions or local municipalities	NO
	Immovable property	SE[175]
	Agricultural, residential and facility leases	SE
	Will	CZ, SE
	Marital agreement	SE
	Contract on sale by instalments	SI
	Construction contract	SI
	Licence agreement	SI

Country-specific examples

In **Cyprus**, some types of contracts are heavily regulated as regards their formalities. For instance, a contract of leasing of immovable property for one year needs two witnesses and signature. Also, a “bond in customary form” (a specific Cypriot contract that works as acknowledgment of debt) also requires two witnesses with their signature. Likewise, transfer of immovable property is heavily regulated in Cyprus. For the transfer of property to occur, the written contract must be registered at the district land office. For the creation of a legal mortgage too, a specific form has to be registered at the district land office. Similarly, for the creation of security on movable property, if the charger is a Cyprus legal entity, it must register the charge with the Registrar of Companies on the prescribed form. Furthermore, any security on a vessel should also be registered at the Cyprus Ships Registry. These heavy regulations can represent a challenge for smart contracts, as the latter may not satisfy the form requirements for specific contracts.

Germany represents an interesting example, as several forms of contracts are foreseen in the national legislation (written form, electronic form, text form, notarial recording, official certification), which are used for specific sectors. For instance, the text form is required for energy supply contracts and contracts with real estate agents. Moreover, when a written form is required by law, a handwritten signature must be provided. If a text form is required by law (or agreed by the parties), it is sufficient if the contract data are transmitted in standard file formats. The presented examples of form requirements in Germany (text form

[174] Sweden does not generally require the use of notaries. Nonetheless, the purchase of real property requires a physical format, and therefore cannot be concluded electronically. The legislative provision does not include the possibility of an electronic signature, but rather assumes a hand-written signature from both seller and buyer. However, the registration of real estate can be completed electronically, provided the required information (e.g. property designation), is included in the application made to the Swedish Mapping, Cadastral and Land Registration Authority (Lantmäteriet).
[175] Ibid.

and written form with a handwritten signature) can be challenging requirements for smart contracts to fulfil.

Another useful example is **Hungary**, as it contains specific requirements for the validity of electronic contracts, which can apply to one type of smart contract. Based on the Hungarian legislation, whether a smart contract can satisfy the requirement of the written form or not, depends on the nature of the smart contract (i.e. whether it is a natural language, hybrid or code-only contract). In particular:

- Natural language contract with automated performance will satisfy such a requirement;
- The fulfilment of this requirement by hybrid smart legal contracts will depend on whether computer code is considered to satisfy the requirement of form in writing;
- A code-only smart legal contract would fall under the special regime of electronic contracts. As noted above in section 3.2.2, for electronic contracts to be considered valid and in force, three conditions on the form/medium in which the statement is expressed must be satisfied cumulatively:
    - It must allow for the retrieval of the original, unaltered content of the statement;
    - It must enable the identification of the person who provided the statement; and
    - It must enable the precise identification of the time when the statement was made.[176]

In the transactions on immovable property in **Norway**, there is no form requirement for the contract, however, the acknowledgement of deeds (in Norwegian, *skjøte)* when transferring real estate is carried out by the Norwegian Mapping Authority[177]. It is the same authority that is responsible for the registry for immovable properties (in Norwegian, *Grunnboken*). The rights registered receive the full legal protection. Similar to the abovementioned examples, the involvement of a public authority can be a challenge for smart contracts.

Form requirements for passive contractual terms

Essentially, the only requirement across all EEA Member States in relation to passive contractual terms (e.g., clauses on liability, choice of law/jurisdiction, statutory clauses) concerns contracts where one of the parties is a consumer. The main requirement in this regard is the need for the trader to set out the terms of the contract in a clear and understandable manner. However, this can be a challenge for the use of smart legal contracts (particularly, ones that are code-only), as the language of code is unlikely to be considered as clear and unambiguous.

Somewhat unique requirements on statutory/mandatory provisions on passive contractual terms are set out in the following EEA Member States (**CY, DE, FI, HR, MT, NL, PT, SI, SK**).

In **Croatia,** the Law on Obligations provides for the limitations of liability if one action has become impossible due to an event for which the debtor is responsible. The obligation is then limited to the remaining action in case the right of choice belongs to him, and if the

[176] It is also argued in the Hungarian national report that as long as hybrid and code-only contracts might satisfy the requirement of a private document with evidentiary power such as electronic documents provided with an electronic signature, the requirement of the written form would be satisfied.
[177] *Kartverket*, https://www.kartverket.no/en/property/transfer-of-property.

right of choice belongs to the creditor, he may, at his choice, demand the remaining action or compensation for damages. In case the action has become impossible due to an event for which the creditor is responsible, the debtor's obligation ends, but in the event that the debtor has the right to choose, he can demand compensation for damages and fulfil his obligation with the remaining action, and if the creditor has the right to choose, he can give compensation for damages and demand the remaining action.

On the basis of the general principles of **Cypriot** contract law, the doctrine of incorporation of terms into a contract requires that the more impact a clause has on the economy of contract (i.e. clause on liability limitation), the more effort must be deployed to give notice to the other party on the existence of this clause.

Although according to **Finnish** law, passive contractual terms are in general free of formal requirements, jurisdiction agreements on the choice of law must be made in writing. In addition, if the parties would like to refer to a specific condition in the contract, for example clauses on liability, it is easier to do so if the conditions are concluded in writing. In case of a dispute, the parties must sufficiently prove the existence of such provisions to appeal to the content in them. Provisions regarding jurisdiction are to be concluded in writing to ensure clarity when referring to them.

In **Germany**, in the case of off-premises and distance contracts, the trader must provide information on the existence of a statutory right of liability for defects in the goods or digital products.

Additionally, choice of law/jurisdiction requires a special form for some contracts. Similarly, in **Portugal** in case of off-premises contracts, the trader must comply with a list of mandatory clauses to be included.[178] In **the Netherlands**, statutory provisions that apply to certain types of contracts to prevent the stronger contracting party from concealing through the inclusion of certain 'cosmetic' terms. These additional requirements may pose challenges to smart contracts. In **Malta**, some provisions are mandatory and cannot be contracted out of, such as, for example, in the case of limitation of liability in cases of fraud, wilful misconduct or gross negligence. In **Slovakia,** the seller (both in B2B and B2C contracts) is responsible for defects that the sold item has when it is taken over by the buyer. In the case of used items, he is not responsible for defects caused by their use or wear. In the case of items sold at a lower price, he is not responsible for a defect for which a lower price was negotiated. If it is a used item, in B2C contracts the buyer and seller can also agree on a shorter warranty period, but not shorter than 12 months**.** Finally, in **Slovenia** a written form of certain contractual terms is stipulated, such as the prohibition on competition after the termination of a commercial agency contract. The written form

[178] These contracts must include clauses with the following contents:
i) Essential characteristics of the good or service, to the extent appropriate to the support used and to the good or service object of the contract;
ii) Total price of the good or service, including fees and taxes, supplementary transport charges, postal or delivery charges or any other charges that may apply;
iii) The method of calculating the price, including everything that refers to any additional transport, delivery and postal charges, and any other costs, when the nature of the good or service does not allow calculation prior to the conclusion of the contract;
iv) An indication that additional transport, delivery and postal charges and any other costs may be due, when such charges cannot reasonably be calculated prior to the conclusion of the contract;
v) The total price, which must include the total costs, per billing period, in the case of a contract of indefinite duration or that includes a periodic subscription;
vi) The total price equivalent to the totality of the monthly or other periodic charges, in the case of a contract with a fixed tariff, and the method of calculating the price must be communicated when it is impossible to calculate it before the conclusion of the contract.
vii) Cost of using the distance communication technique, when calculated with reference to a tariff other than the base tariff;
viii) The existence of relevant codes of conduct, if any, and the way to obtain the respective copies.

requirement does not in itself hinder the use of smart legal contracts, as a contract in electronic form can meet the requirements of a written form.

Smart legal contracts equated to prose (written) contracts

There are no rules equating smart legal contracts with prose contracts with written or electronic signatures in 23 EEA Member States (**AT, BE, BG, CZ, DE, DK, EE, FI, FR, HR, HU, IE, IS, LI, LT, LU, LV, NO, MT, NL, PL, RO, SK**). The rules on other types of contracts can, thus, be applied to smart contracts by analogy. The laws of two of the remaining seven EEA Member States (**GR**[179]**, IT**[180]) contain such provisions, whereas the other four EEA Member States (**ES, PT, SE, SI**) have provisions which equate *electronic* contracts to prose (written) contracts. In one EEA Member State (**CY**), a draft DLT law stipulates that smart legal contracts have to be regarded as written contracts.[181]

The **Greek** legislation stipulates that where a signature or seal is required for the conclusion of a smart contract, it may be placed in the form of an electronic signature or an electronic seal. Additionally, the **Italian** legislation only provides that smart contracts satisfy the requirement of the written form, upon prior IT identification of the interested parties, meeting the Agency for Digital Italy (AGID) requirements, following its guidelines.

In four EEA Member States (**ES, PT, SE, SI**) while no specific provisions exist on smart contracts, provisions equating electronic contracts to written (prose) contracts exist. Particularly, according to the **Portuguese** laws, the electronic document is valid as a signed document when it meets the requirements of the legislation on electronic signature and certification.[182] Moreover, as per the **Slovenian** legislation, a contract written in electronic form (which can include computer code) is equivalent to a written (prose) contract if the content of the contract can be read from the code using a computer. However, an exception to that rule applies to certain types of contracts, which have higher stricter formality requirements (e.g., contracts which have to be concluded in the form of the notarial deed).[183] The **Spanish** legislation similarly equates electronic contracts with written contracts: whenever the law requires that the contract or any information related to it be in writing, this requirement shall be understood to be satisfied if the contract or the information is contained in an electronic medium.[184] Finally, in **Sweden** very few provisions on contract type are found in the legislation, hence the contract form (oral, written, electronic etc.) does not generally affect legal validity, as the same underlying rules apply for an agreement to be legally valid. In addition, where a written document or signature is required, this should generally be possible electronically.

Requirements on durable mediums for consumer contracts

[179] Article 50 of Law 4961/2022 on Emerging Information and Telecommunications Technologies, enhancement of digital governance and others.
[180] The second part of par. 2 of Article 8-ter of Decree no. 135 of 14 December 2018 provides that smart contracts satisfy the requirement of the written form, upon prior IT identification of the interested parties, meeting the Agency for Digital Italy (AGID) requirements, following its guidelines, thereby equating smart contracts to written contracts.
[181] Proposal related to distributed ledger technology (“DLT draft law”), Article 12). The text in English is available at: https://mof.gov.cy/assets/modules/wnp/articles/202109/949/docs/dlt_bill_en_for_public_consultation.docx.
[182] Article 26, para 1 of Decree No. 7/2004,
available at: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1399&tabela=leis&so_miolo.
[183] Art. 13, para. 2 Electronic Business and Electronic Signature Act (*Zakon o elektronskem poslovanju in elektronskem podpisu*).
[184] Article 23 of Law 23/2002.

Twelve EEA Member States (**AT,**[185] **BG, CY, EE, DE, IE, IT,**[186] **LI,**[187] **MT, NL, SI, SK**[188]) deal with the notion of *durable medium* by providing a definition for it, which stems from Article 2(10) of the Consumer Rights Directive (CRD) and is either transposed verbatim or somewhat altered.[189] In seven EEA Member States no specific requirements or provisions on durable mediums exist (**CZ, FI, GR, HU,**[190] **IS, LT, LV**[191]), while specific requirements exist in eleven EEA Member States (**BE, DK, ES, FR, HR, LU, NO, PL, PT, RO, SE**).

In **Belgium**, the requirement of a writing is satisfied by a set of alphabetical signs or any other intelligible signs affixed to a medium which allows access to it for a period of time appropriate to the purposes for which the information is intended and which preserves its integrity, regardless of the medium and the means of transmission (Civil code, Article 5.30).

Similarly, in **Luxembourg**, the requirement of a writing is satisfied by a set of alphabetical signs or any other intelligible signs affixed to a medium which allows access to it for a period of time appropriate to the purposes for which the information is intended and which preserves its integrity, regardless of the medium and the means of transmission. Additionally, the electronic private document is valid as an original when it presents reliable guarantees as to the maintenance of its integrity from the moment it was first created in its final form (Civil code, Article 1322-2).

The **Croatian** Law on consumer protection provides for the obligation to use durable medium in case of written complaint of the consumer, while the trader should store records of written consumer complaints on a durable medium for one year from the date of receipt of the written consumer complaint.

As a general rule, there are no requirements regarding ‘durable mediums’ in **Denmark**. However, in specific situations, such as proof of ownership of an asset, in case of loans,

[185] The Austrian Supreme Court (OGH) ruled that such a durable medium may also be a website if the data retrievable there can be viewed unchanged for a period of time appropriate for the purposes of the information (4Ob 58/18k). https://www.ogh.gv.at/entscheidungen/entscheidungen-ogh/zum-begriff-des-dauerhaften-datentraegers/.

[186] The Italian legislation also states that the consumers are not bound by the contract until they give their written consent, provided that such confirmations may also be made on a durable medium.

[187] According to the EFTA-Court judgment of 27.1.2010, an internet website can be classified as a "durable medium" if it enables the consumer to store the information referred to in Article 12 of the Directive 2002/92/EC and in such a way that it can be accessed unchanged and for a reasonable period of time, i.e. for as long as is necessary for the consumer to safeguard his interests (E-4/09). https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:E2009J0004&from=HR.

[188] Within Slovak consumer law, rules that a durable medium is capable of replacing a written contract (e.g. as an electronic contract on a durable medium), or that the information obligation may be met by providing a consumer with information on a durable medium.

[189] 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:32011L0083.

[190] There are no Hungarian *sui generis* rules on a durable medium in the Civil Code. The rules on durable mediums are provided in statutes implementing EU law, such as Section 6(1)(1) of Act CLXII of 2009 on Consumer Credit implementing Directive 2008/48/EC on Consumer Credit.

[191] There are no types of contracts for which the use of durable medium is explicitly excluded as a possibility. The law does not explicitly exclude certain types of agreements from possibility to use a durable medium. In fact, even reference to the requirement to conclude a contract in writing is expressed as a possibility to do this “on paper” or via a durable medium. For example Article 11(7) of the Consumer Rights Protection Law provides: “A contract on the right of use of accommodation, a contract on holiday services, a resale contract, and an exchange contract shall be concluded in writing (on paper or on another durable medium) and one copy of such contract shall be issued to the consumer at the time of concluding the contract.”

property, a requirement of e-signature or a 'durable medium' may be imposed/required by law.[192]

In **Iceland**, Article 15(1) of Act No. 118/2016 on Real Estate Loans to Consumers for example requires credit intermediaries to provide specific information about themselves to consumers before offering their services on paper or a durable medium.[193] Moreover, agreements on real estate loans shall be registered on paper or a durable medium according to Article 16 a. Similar provisions can be found in Act No. 33/2013 on Consumer Loans on information provided by the lender to consumers before a loan is given, cf. Article 7(2).[194] According to Article 12(1), loan agreements shall also be registered on paper or a durable medium. Similar provisions can also be found in Act No. 16/2016 on Consumer Contract's[195] (see Articles 7 – 9) and Act No. 115/2021 on Markets for Financial Agreement's (e.g., Article 46 and 51).[196]

No specific requirements exist directly in the **Norwegian** legislation. However, some specific laws (for example, Archive law[197] or Accounting law[198]) may in practice introduce those in relation to the proof of transaction.

In **Portugal**, the contractual terms and general clauses, as well as the acknowledgment of receipt, must always be communicated in a way that allows the recipient to store and reproduce them.

The **Spanish** legislation requires to deliver to the consumer a printed copy of the contract or on a durable medium, so that when there is a discrepancy between the content of the computer code and the version delivered to the consumer, the latter will prevail, which is the one on which the consent has been issued. An additional requirement applies in the cases of telephone or electronic contracting, according to which it will be necessary to state in the terms established by law the acceptance of each one of the clauses of the contract, without the need to conventional signature. In this case, the consumer will be sent a written justification of the contracting carried out, where all the terms of the same will be stated". According to some authors, the referral of the contract made does not necessarily have to be done on printed paper, being sufficient, for example, by email, since what is sought, fundamentally, is proof of the contract made.[199]

In **Sweden**, there are no specific requirements regarding durable mediums, as the Swedish government's aim was for such provisions to be as flexible and efficient as possible, by including such possibilities as post, e-mail and sms.[200] While the national law does state that particular consideration must be given to the needs of minors and other

[192] Legal source: Betænkning nr. 1400/2000 (https://www.betænkninger.dk/wp-content/uploads/2021/02/1400.pdf); Lovbekendtgørelse nr. 669 af 23. september 1986 af lov om gældsbreve (https://www.retsinformation.dk/eli/lta/1986/669); Lovbekendtgørelsenr.1490 af 23. december 2014 af Lov om ændring af lov om finansiel virksomhed, lov om værdipapirhandel m.v., lov om betalingstjenester og elektroniske penge og forskellige andre lovehttps://www.retsinformation.dk/eli/lta/2014/1490

[193] The Act on Real Estate Loans to Consumers can be found here: https://www.althingi.is/lagas/nuna/2016118.html

[194] The Act on Consumer Loans can be found here: https://www.althingi.is/lagas/nuna/2013033.html

[195] The Act on Consumer Contract's, available at: https://www.althingi.is/lagas/nuna/2016016.html

[196] The Act on Financial Agreement's, available at: https://www.althingi.is/lagas/nuna/2021115.html

[197] Lov om arkiv [arkivlova] - Lovdata of 04.12.1992.

[198] Lov om årsregnskap m.v. (regnskapsloven) - Lovdata of 17.07.1998.

[199] Legerén-Molina, A. (2018) 'Los contratos inteligentes en España. La disciplina de los Smart contracts' Revista de Derecho Civil. Available at: https://www.nreg.es/ojs/index.php/RDC/article/view/320.

[200] Government Bill 2017/18:128 p.31-32 [Prop. 2017/18:129 Skriftlighetskrav vid telefonförsäljning]. When legislation was being prepared, some authorities did question the appropriateness of sms as a medium due to the practical limitations of space constraints; other authorities questioned the appropriateness of both sms and email, for reasons of security but also due to regulations limiting the use of such communications e.g. within the financial sector.

vulnerable people, its focus here is on the clarity of the information itself, rather than the medium through which it is given.

It can be seen from the abovementioned analysis that, in the EEA Member States where specific legislation exists on the issue, a durable medium in consumer contracts is mostly used to satisfy the requirement of the written form. Durable mediums are also often noted as a possible alternative to a paper copy of a contract. In this light, smart contracts could potentially be used as durable medium under the Consumer Rights Directive.

Challenges

Overall, the requirements of specific forms in the law (such as requirements of notarial authentication or registration with public authorities) can constitute a challenge for smart contracts where they cannot be satisfied by smart legal contracts. In addition, the particular requirements related to consumer contracts (for instance, the requirement of setting out the terms of the contract in a clear and understandable manner) can constitute a challenge for smart legal contracts, as the language of code may not be considered clear and comprehensible.

3.2.4. Contract interpretation/evidential value

Rules of interpretation and potential challenges

Rules of interpretation of contracts were found in all EEA Member States. Legal experts in five EEA Member States (**AT, GR, LI, LT, SI**) did not point out any potential challenges for smart contracts stemming from the rules of interpretation in their national legislation. In most EEA Member States, the rules of interpretation are incorporated into civil codes. At the same time, eleven EEA Member States (**BG, CY, DK, EE, FI, HR, IE, IS, NO, SE, SI**) have separate acts and/or existing case law regarding contract law, which lay down the interpretation rules.

It is important to note that EU consumer law harmonised national laws on B2C level and Member States have transposed these rules into their domestic laws. Therefore, according to Directive 93/13/EEC[201], the interpretation most favourable to the consumer prevails in case of doubt about the meaning of a contract term[202]. Furthermore, the same Directive also lays down that a contract term must be assessed by referring, among others, to all the other terms of the contract, as well as to all the circumstances attending the conclusion of the contract.[203] A separate section (3.2.5) elaborates further on EU consumer law, as these are relevant challenges in all EEA Member States. In the following paragraphs, challenges raised by national legal experts regarding contract interpretation and evidential value related to smart contracts are also discussed.

In terms of rules of interpretation, several similarities appear across the EEA Member States. The most frequently recurring rules of interpretation are (as harmonised by Directive 93/13/EEC):

[201] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.
[202] Article 5 of Council Directive 93/13/EEC.
[203] Article 4 (1) of Council Directive 93/13/EEC.

- the intention of contractual parties in the cases when interpreting the wording of an agreement raises doubts;
- the obligation to read contractual provisions in conjunction with the whole agreement;
- to take into consideration accompanying circumstances.

Further interpretations rules in place include, for example:

- good faith (**BG, DE, ES, GR, IT, LT, PT, SE**);
- common practice (**BG, DE, LT, MT, SK**);
- precontractual negotiations (**EE, IS, IT, LT, SE, SK**);
- purpose of the contract (**CZ**, **DE, EE, PL**);
- linguistic interpretation (**CZ, IE, LV, SK**).

Regarding the challenges posed by rules of interpretation to smart contracts, similarities have been identified by legal experts across EEA Member States. Firstly, a potential challenge indicated by legal experts in several EEA Member States (for example, **BE, BG, CY, CZ, DE, DK, EE, ES, FR, HR, IE, IS, IT, MT, NL, LU, LV, NO, PT, RO, SE, SK**) concerns the fact that in case of smart legal contracts, extracting information on the intention of the parties, especially non-objectively assessable elements is arduous and requires further technical innovation. For example, certain phrases such as 'best efforts', 'good faith' or 'reasonable period' are open to interpretation and require evaluation on a case-by-case basis. In other words, compressing subjective phrases into computer codes contradicts the nature of these indeterminate legal terms, as they are applied so that contracts can endure in individual circumstances. At the same time – according to legal experts – potential solutions to overcome this challenge might exist (for example, **DK, FI, IE**), for instance, by avoiding ambiguity and putting emphasis on precise provisions in a smart contract (for example, **FI**), or by making background materials (including content of pre-contractual negotiations) accessible could also counterbalance the interpretation hurdles created by smart contracts (for example, **DK, IE**). Additionally, German scholars (such as *Sebastien Schnell* and *Corbinian Schwaab*) argue that smart legal contracts, which are based on the same program code and are used on a larger scale, are similar to standard business terms and parties become familiar with their content. Therefore, they could be easily applied.[204]

Secondly, a closely related challenge to interpreting the intention of the parties is the difficulty of adding specific elements to an agreement, underlined by legal experts in some EEA Member States (for example, **BE, DE, FR, LU, PT**). The challenge here is that the computer code cannot integrate certain individual provisions in the smart legal contract itself (for example, the expected characteristics and nature of a good sold). Such individual provisions would still require human interpretation for an agreement to be concluded.

Thirdly, legal experts in some EEA Member States (for example, **HU, IE, NL, PL, PT, RO, SE, SK**) flagged that the lack of technical expertise (both on the side of interpreters of law [i.e. courts] and for parties of an agreement) can lead to complications in comprehending code language (e.g. interpreting provisions of an agreement or giving valid consent to an agreement).

Requirements of full evidential value and potential challenges

[204] Schnell, S. And Schwaab, C., Vertragsgestaltung beim Einsatz von Smart Contracts zur Automatisierung von Lieferbeziehungen, Betriebs-Berater, 2021. Available at: https://www.hoganlovells.com/-/media/germany_folder-for-german-team/artikel/2021_schnell_schwaab_betriebsberater_19_2021_smart-contracts.pdf.

National legal experts from the following EEA Member States (**AT, BE, CY, GR, FR, HU, IE**[205]**, IT, LI, LU, LT, MT, NL, PL, PT, RO**) have indicated requirements concerning full evidential value in the context of (court) claims. Among these EEA Member States, five (**FR, HU, IT, LT, NL**) indicated to have rules in place regarding the condition of clear identification as a requirement for full evidential value. Moreover, in three cases (FR, IT, NL) it was flagged that rules on storage conditions with which documents need to comply in order to have full evidential value exist. 14 EEA Member States (**AT, BE**, **CY, FR, GR, HU, IT, LI, LU, MT, NL, PL, PT, RO**) have specific rules on full evidential value, which require further elaboration below. In the remaining 14 EEA Member States, no regulations on full evidential value were detected (**BG, CZ, DK, DE, EE, ES, FI, HR, IS, LV, NO, SE, SI, SK**).

Most legal experts in EEA Member States with rules on full evidential value in place have indicated possible challenges, except five (**BE, DK, GR, HU, LU**). The most common challenge detected by legal experts is related to the interpretation of the language of smart contracts (**FR, MT, RO**) which in general is vital for an agreement to have full evidential value. Other challenges indicated by the legal experts are EEA Member State-specific and, therefore, are described in detail below.

It should be noted that legal experts in 5 EEA Member States (**FI, IS, LV, NO, SK**) without rules on full evidential value (in their case, the court decides on evidential value) nonetheless indicated that judges could face challenges when deciding on the evidential value of smart legal contracts.

In **Austria,**[206] public documents (either in paper or electronic form) issued by a public authority or by a person vested with public trust within the scope of their business bear full evidential value. Applying smart legal contract infrastructure in these areas could be challenging. On the one hand, it is uncertain if the identification and verification of the authority issuing the public document would be possible in case of smart contracts. On the other hand, it is questionable if smart contracts could display essential form requirements of public documents (e.g., official stamp). These rules and challenges also apply to **Liechtenstein**[207].

In case of **Belgium**, the principle of free evidence exists, which means that proof may be provided by any means.[208] Nevertheless, legal arrangements involving a sum or value exceeding EUR 3,500 bear full evidential value if incorporated in a written document, signed by the parties.[209] Furthermore, the Belgian Civil Code lays down that only signed documents can serve as counter proof against another signed document. The same rules exist in **Luxembourg**[210], with the following difference. In Luxembourg, legal arrangements involving a sum or value exceeding EUR 2,500 bear full evidential value if incorporated in a written document or registered by a notary.

In **Cyprus**, based on the ‘parole evidence rule’ of common law, a contract in written form is recognized as having full evidential value. A challenge could occur, if in parallel with a smart contract (based on coding), a natural language version also exists. The question is,

[205] According to Article 22 of the Electronic Commerce Act of 2000, electronic contracts, electronic communication and electronic signatures have full evidential value.
[206] Article 292 (1) of the Civil Procedural Code of Austria (ZPO).
[207] Article 292 (1) of the Civil Procedural Code of Liechtenstein (ZPO).
[208] Article 8.8 of the Belgian Civil Code.
[209] Article 8.9 of the Belgian Civil Code.
[210] Article 1341 of the Civil Code of Luxembourg.

which version of these two would prevail as stronger evidence (thus having full evidential value).

As mentioned earlier, **Greece** has a recently adopted legislation in force for smart contracts.[211] Based on the Greek law, smart contracts have full evidential value, if a report by an expert in science of cryptography on the smart contract is presented, along with its electronic code. Moreover, the content of the smart contract embedded in the electronic code must be depicted in an intelligible language (Greek or other language).

In **France**, the legislator lays down equivalent rules on the full evidential value of non-digital and digital documents, as long as the origin of the digital document is duly identifiable (i.e. from whom which natural or legal person it emanates from) and if the digital document is drafted and stored under conditions guaranteeing its integrity.[212] In practice, these conjunctive conditions for digital documents are ensured by using electronic signature in online transactions. The challenge for smart contracts in the French legal system is that the automated nature of the verification of compliance with the terms of the contract (formulated in lines of code) leads to a situation where no written proof of agreed rights and obligations of the parties exist, questioning their ability to have evidential value. Furthermore, to understand how terms and conditions of the smart contract are formulated and applied – and thus be used as evidence - requires technological knowledge.

The **Hungarian** Civil Code[213] distinguishes between three types of documents in terms of evidential value. Firstly, 'public documents' are issued by public authorities and have an irrebuttable presumption of truth. Secondly, 'simple private documents' have no formal requirements, and their evidential value is subject to the court's evaluation. The third category are 'private documents with evidentiary power', which have a rebuttable presumption of truthfulness of their content and of the intention of the parties. To fulfil the requirement on evidentiary power, these types of private documents must be signed by the parties and prepared by lawyers. Moreover, since 2021, certain contracts made via electronic means are only valid and enforceable if their content is displayed with graphemes and satisfies the requirements for electronic documents, namely ensuring that an advanced electronic signature is provided. This allows the verification of the authenticity and originality of the content of electronic documents.

In **Italy**, documents in electronic form must comply with the Code of Digital Administration (CAD).[214] According to the CAD, an electronic document has full evidential value, if signed with a qualified digital signature or an advanced electronic signature. Furthermore, the Italian legislation regards smart contracts as electronic documents (as defined under Article 3(35) of the eIDAS definition). Therefore, smart contracts can have full evidential value, only if they have a qualified digital signature or an advanced electronic signature (as laid down in the eIDAS regulation) or a digital signature (the latter is a special category in Italian law and consists of a qualified electronic signature that uses asymmetric cryptography). Concerning smart contracts, an important provision in Italian legislation is that the previously mentioned evidential value is recognised to documents formed under the requirements set by the Agency for Digital Italy (AGID),[215] prior to the IT identification of its author. The conditions for this are twofold. Firstly, the security, integrity, and immutability of these documents must be guaranteed, and they need to clearly and unequivocally be

[211] Law 4961/2022 on Emerging Information and Telecommunications Technologies, enhancement of digital governance and others.
[212] Article 1366 of the French Civil Code.
[213] Act V of 2013 on the Civil Code.
[214] Article 20 of the Code of Digital Administration (CAD).
[215] Article 71 of the Code of Digital Administration (CAD).

ascribable to their author. Therefore, the main challenge in terms of evidential value could be created by uncertainties surrounding the identification of the signatories.

In **Malta**, the evidential value of documents is based on the best evidence rule. According to this rule, the original agreement or a certified true copy of the agreement should be filed if someone wishes to ensure a document has full evidential value. In some cases, documents require notarisation or an apostille to bear full evidential value. There are no specific rules in relation to smart contracts. However, where ITAS certification is necessary for a document[216], both a dry code (i.e. purely electronic format of the contract) and a wet code (i.e. English language statement) must be provided for full evidential value. If there were a discrepancy between the two codes, the wet code prevails. As things stand, a relevant challenge for the application of smart contracts could be related to the interpretation of such contracts in the absence of 'write everything twice' (wet) codes.

In the **Netherlands**, the law does not differentiate between the evidential value of non-digital and digital documents. If the law requires a document to be in written form, the electronic document must be stored in an accessible way (for a period appropriate to the purpose for which the instrument is intended to serve) and must ensure the unaltered reproduction of the contents of the document. Furthermore, electronic documents require an electronic signature to have full evidential value. It should be noted that there is no specific rule for smart contracts in the Netherlands, but rules on electronic documents could apply to them. A challenge regarding full evidential value is that courts have freedom in evaluating evidence and hence how far a smart contract in the subjective scrutiny of a court can have evidential value. At the same time, the outcome of the deliberation and the process leading to the decision of the court must be justified in the court's judgement. By this, arbitrariness and legal uncertainty can be avoided.

In **Poland**, agreements with a notarial deed and private documents maintaining the written form agreed by the parties and holding their signature have full evidential value. According to the Polish Civil Code,[217] electronic documents need a qualified electronic signature for full evidential value. Other forms of legal act, even when in writing, but without these requirements cannot bear full evidential value. The current Polish legislation raises challenges for smart contracts as it is unclear whether they could be fulfilling the requirements for the written form.

In **Portugal**, public documents issued by authorities (by a notary or other public official) and private documents confirmed by parties before a notary bear full evidential value.[218] As a consequence, smart contracts would not have full evidential value without the required certification of a public official.

In **Romania**, written documents can have full evidential value. In certain cases, witnesses can prove the existence of a contract in case the subject of the contract does not exceed RON 250.[219] This value restriction is absent in case contracts are used as evidence against professionals. However, in such cases Romanian law can require specific written evidence. In Romania, the identified challenge is related to the comprehension of code language. As

[216] Innovative Technology Arrangements and Services Act (ITAS Act).
[217] Article 78 of Act of 23 April 1964 on the Civil Code.
[218] Articles 371, 376 of the Portuguese Civil Code.
[219] Romanian New Leu.

smart contracts are created as lines of codes, it is questionable if courts would be able to interpret smart contracts and thus consider them as documents with evidential value.

Challenges

In summary, contract interpretation rules are significantly influenced by EU consumer law, but some other, more EEA Member State specific interpretation rules also exist. Challenges in this field are mostly similar. More precisely, the most frequent challenges in the framework of interpretation are related to the immutable nature of smart contracts, as well as to specific elements, in which case objective assessment is difficult. In terms of full evidential value, half of the EEA Member States have rules in place. The most common challenges in the EEA Member States show a larger variation. Challenges in this field include fulfilling formal requirements, as well as specific rules on certain types of documents.

3.2.5. Consumer law requirements

Consumer protection law acts in commercial transactions to protect the weaker party against the stronger party. In the data economy there is an obvious need to safeguard the protection of weaker parties, such as consumers, in light of prevailing power asymmetries. These protections appear to be more important in contexts where technologies with potentially irreversible outcomes, such as blockchains and smart contracts, are used as algorithmic decision-making casts doubt on the foundational paradigm of EU consumer law, namely consent (note, however, the difference between consent in data protection and consumer protection law) and autonomy.[220] Article 30 of the draft Data Act addresses these concerns, but of course consumer protection law also applies. It is important to stress that the draft Data Act would be without prejudice to consumer protection law.[221] As a consequence, consumer protection law must be respected whenever data is exchanged between parties qualifying, respectively, as consumers and traders, in the context of the draft regulation's portability regime. Indeed, although consumer protection law applies in such settings, it does not restrict access to and sharing of personal and non-personal data as such. Nonetheless, the Unfair Contract Terms Directive (UCTD),[222] the Unfair Commercial Practices Directive (UCPD)[223] and the Consumer Rights Directive (CRD) protect consumers by banning specific unfair commercial practices.[224] These are horizontal norms applicable across sectors and hence also applicable in the context at hand.

The Definition of Consumer

To determine the applicability of consumer protection law, it first needs to be determined whether there is a relationship between a consumer and a trader. This raises the question of the definition of the consumer under EU law. Although different consumer protection

[220] Mateja Durovic and Franciszek Lech, A Consumer Law Perspective on the Commercialization of Data (2021) 29 European Review of Private Law 701-732.

[221] See, inter alia, Article 2(6) of Directive 2019/779/EU.

[222] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L 95.

[223] 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.

[224] 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, 22.11.2011, p. 64–88.

instruments employ slightly diverging interpretations of this term, we can use one of the most recent definitions (more recent definitions present more similarity) to determine when a data user is a consumer. EU law defines the consumer as the natural person who is acting for purposes that are outside that person's trade, business, craft profession.[225]

Information Requirements for Consumers

Under EU consumer protection law, consumers are legally entitled to pre-contractual information (and sometimes an accompanying reflection period) during which the contract cannot yet be considered to have been concluded and performance thereof may not yet begin. In cases where the data holder also qualifies as a trader under EU consumer protection norms, they are bound by applicable supranational consumer protection instruments.

The CRD requires that specific information be provided in relation to consumer contracts.[226] Its Article 5 CRD mandates that the consumer be informed about the main characteristics of the goods and services, 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[227] furthermore requires that recipients of a service must be provided with information regarding: 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; and (e) where the activity is subject to an authorisation scheme, the particulars of the relevant supervisory authority.

Furthermore, according to Article 10 of the 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; and (d) the languages offered for the conclusion of the contract. It follows that where there is a contract between data holders and data users, as is for instance the case where data sharing occurs under Article 4(6) of the draft Data Act, and the data holder and user respectively qualify as traders or consumers, consumer protection law applies. It has been criticised that legal persons enjoy better protection under the draft Data Act compared to natural persons (unless they also qualify as a business) in their capacity as consumers given that the latter only benefits from specific protections where consumer protection law, in particular the Unfair Contractual Terms Directive,[228] applies whereas the former always enjoy the protection of Article 13 of

[225] See, inter alia, Article 2(6) of Directive 2019/779/EU.

[226] 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, 22.11.2011, p. 64–88.

[227] 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.

[228] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L 95.

the draft Data Act, which prohibits unfair terms in contracts between enterprises.[229] It has indeed been argued that 'there is no reason to believe that Articles 13(3) and 13(4) is not appropriate to be applied to B2C contracts as well'.[230]

The national rules transposing the abovementioned EU-level provisions are stipulated in the national laws in all EEA Member States. However, two EEA Member States' laws (**DE, NO**) also contain additional notable provisions. In **Germany**, a court case that could be applied by analogy to smart contracts is the case of Amazon Dash buttons,[231] where the Higher Regional Court Munich banned these buttons because they did not inform consumers sufficiently about the ordered goods and the price. In **Norway**, the information provided to consumers shall be presented in Norwegian.

In this regard, it should be noted that challenges can arise in relation to the information requirements under consumer law, as these need to be in a clear, specific and understandable manner to ensure that the consumer can fully understand their meaning. In addition, the requirement to provide the pre-contractual information on a durable medium in the case of distance contracts can also be challenging. Moreover, the expression of the will of the parties in lines of code may not always suffice to ensure the parties' consciousness and intent to conclude a contract, and there is a need for specific approval in writing or giving evidence of individual negotiations. Finally, the privacy and use of personal data can be a challenge for smart contracts. The transparent nature of the blockchain and the possibility for all the nodes in the network to access the database containing the smart contract could potentially pose a problem in view of the personal data and privacy protection, notably not only for consumer contracts but also for business contracts.

Indeed, pursuant to the principles of technological neutrality and functional equivalence, the requirements emerging under consumer protection law also need to be respected where technical tools such as smart contracts are used. The existence of consumer rights should not, and as a matter of law does not, hinge on what technology is used, including whether this technology uses a smart contract.

In all EEA Member States, consumer law requirements are applicable to smart contracts. In this light, the information requirements imposed on traders apply to smart contracts as well and can pose some challenges to smart legal contracts (which is discussed above in section 3.2.3). Particularly, the use of the mere language of the code to express contractual terms may not be enough to comply with consumer protection rules, including the consumer's right of withdrawal. Nonetheless, such clauses could be coded within the smart contract in a way to be in line with regulations. Moreover, depending on the specific type of service or field of contract there may be additional requirements for consumer contracts that must be complied with. Finally, "the volatility of certain cryptocurrencies also poses a threat to the certainty of the execution of the contract."[232]

As an example of language requirements, the **Slovenian** legislation can be mentioned. According to it, a specific requirement that needs to be taken into account is the provision

[229] Louisa Specht-Riemenschneider, Der Entwurf des Data Acts https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Dateien/MMR-Beilage.pdf,page 817.

[230] Position Statement of the Max Planck Institute for Innovation and Competition, No. 22-05, 48.

[231] Oberlandesgericht München, Urteil vom 10.01.2019 - https://openjur.de/u/2297475.html.

[232] Mentioned in the Cypriot national report.

requiring the companies to do business with consumers in the Slovenian language.[233] In so doing, the company must use its full title and registered address in any written communication. However, these requirements on the use of natural language (Slovenian and, where relevant, Italian and Hungarian) can in principle also be met by smart legal contracts.

Smart contracts are written in computer code. Where a smart legal contract is concluded between businesses, parties can agree that the contractual language is a programming language such as Solidity or Rust. Consumer contracts, however, always also need to be made available in a natural language to enable the consumer to understand what rights and obligations they agree to. For instance, Article 5 of the Directive on Unfair Contract Terms provides that in 'the case of contracts where all or certain terms offered to the consumer are in writing, these terms must always be drafted in plain, intelligible language. Where there is doubt about the meaning of a term, the interpretation most favourable to the consumer shall prevail.'[234]

The Right of the Consumer to Withdraw from a Contract

Article 9 of the CRD stipulates the right for the consumer to withdraw from a distance or off-premises contract (which online contracts intermediated by PIMS can be considered to be) within a period of fourteen days '*without giving any reason, and without incurring any costs other than those provided for in Article 13(2) and Article 14'*.[235] If a contract is concluded under the draft Data Act that binds a trader and a consumer this rule also applies to data sharing. This fundamental consumer right seems at odds with one of the proclaimed benefits of smart contracts, namely their hard-to-reverse nature. Yet, the right to withdrawal does not require that the original, smart contract enabled, transaction is reversed, rather that its effects are. As such, reverse transactions enabled by a new smart contract could be used to give practical effect to the right of withdrawal, a solution that has also recently been endorsed by the European Law Institute.[236] This mechanism could be explicitly anticipated in model contractual terms and the technical implementation thereof could be ensured through interoperability standards that make sure that a request for withdrawal addressed to the trader is also implemented by the party that the data may already have been shared with.

Unfair Contract Terms

Unfair non-individually negotiated contractual terms in B2C contracts are deemed null and void, as set out in Article 6 of Directive 93/13/EEC (UCTD).[237] However, if the other parts of an agreement can be enforced without the unfair terms, the remaining scope of the contract shall remain in force.

However, it should be noted that the UCTD sets out a minimum harmonisation, protecting consumers in the EU from unfair terms and conditions which might be included in a non-individually negotiated contract for goods and services. Moreover, it was developed in the late 1990s, before the *en masse* development of the internet and related technologies. As

[233] In the areas of autochthonous settlement of the Italian or Hungarian national communities, they must also do business in the language of the respective national community.
[234] Article 5 of the Directive on Unfair Contract Terms.
[235] Note that this right does not apply where the exceptions listed in Article 16 of the Consumer Rights Directive apply.
[236] European Law Institute, 'ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection' (European Law Institute 2022), 41.
[237] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L 95.

a technology-neutral Directive, the UCTD applies to all contract terms, regardless of whether the service at the centre of the contract is digital or not. In this light, examples of national provisions transposing the Directive from some EEA Member States are presented below.

In **Croatia**, Articles 49-56 of the Law on Consumer Protection and court practice can help in assessing whether a particular provision can be considered unfair, whether a given contractual provision is impermissible and what are the consequences of the impermissibility of a contractual provision. A person who has an interest in determining the invalidity of certain provisions of the general conditions of the contract can request court protection by filing a lawsuit to determine the invalidity.

In **Estonia**, the provision on unfair terms (not negotiated individually and not influenced by the consumer) provides an extensive list of examples of unfair standard terms in the context of a contract where the other party is a consumer. The Article lists a total of 35 (subsections 1-37 out of which two have since been repealed) separate examples of unfair standard terms. However, it should be noted that these terms are presumed to be unfair in contracts relating to economic or professional activities i.e. even when the other party is not a consumer. Therefore, the list of unfair standard terms can represent a challenge to smart legal contracts, as these are often reliant on terms that will be deemed standard terms. Nonetheless, the aim of consumer protection sought by such a list should be borne in mind.

In **Romania**, the court shall compel the trader that drafted contracts with unfair terms to amend all adhesion contracts in course of being performed and to eliminate the clauses from the contracts that follow to be concluded. Such a contract shall not produce any effects in respect to the consumer, and the contract shall continue to be performed, with the consent of the consumer, only if its performance can still take place after the clauses are eliminated.

In **Sweden** (as well as in all other EEA Member States), the contractual terms that are deemed unfair by a court are no longer valid, as per Article 6 of Directive 93/13. These terms will either be void and unenforceable or adjusted by the court in order to remove the unfairness of the particular clause. In general, the treatment of such unfair clauses or contracts poses the same challenges to smart contracts as any other form of contract. One potential challenge is in relation to contract adjustment in more practical terms. A court can alter contract clauses to ensure fairness between the parties, but this may be more difficult to do in practice in a smart contract. Although not a challenge particular to the Swedish legal system, it is an aspect to consider when employing smart legal contracts.

Challenges

The requirement connected with the identification of the parties to the contracts,[238] the requirement for the trader to set out the terms of the contract in a clear and understandable manner[239] and the execution of the right to withdraw from the contract within 14 days may be challenging to implement in smart contracts (as noted for instance in section 3.2.2). It

[238] Moreover, exceptions from any lack of requirements in terms of identification of the parties apply in relation to Directive 2015/849 in all Member States, as according to Article 13(1)(b), Member States shall establish customer due diligence measures which should comprise “identifying the beneficial owner and taking reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is.”

[239] For further details, see section 3.2.3.

was stated in the legal scholarship[240] that "given that the list of listed, public, without permissions blocks, as the foundation of a smart contract, guarantees the immutability of the transaction, special attention must be given to the technical implementation of the annulment or reversal of an operation." In general, reversal to a prior state of a blockchain is possible by using reversed transactions.[241] However, the operation does not lead to the deletion of the history of transactions, which means that, the reversed transaction remains documented permanently in the blockchain. From a contractual law perspective, this does not raise any issues, but problems may arise concerning the protection of personal data. Moreover, the performance of a reversed transaction may pose challenges, because it may be activated by the owner of the private key. Nonetheless, as discussed above, the right of withdrawal does not require that the original, smart contract enabled, transaction is reversed, rather that its effects are.

The main challenges in this regard are the immutability of the blockchain[242] (as the invalid contract or the invalid clauses can continue to self-execute, and reversing the effects may be difficult) and the interpretation of what is to be considered an unfair term (if no specific provisions are available in the national laws). As the contract should continue without this term, it means that a mechanism should exist that would "deactivate" in the code the specific term.[243] The CJEU case law on unfair terms is relevant in this regard and particularly, it should be noted that the recent CJEU judgment on loans in foreign currency[244] states that in the event that the contract is invalid and it is not possible to re-establish the situation existing prior to its conclusion, the national court must restore the contractual balance between the parties without however going "beyond what is strictly necessary to that end."[245] In other words, an obligation exists according to which the consumer must be restored to the situation that he/she would have been in if the unfair term had never existed. "In the context of smart contract whereas the unfair term cannot be revoked, it entails that the extracontractual liability of the professional is engaged for professional negligence, for the insertion of a known unfair term in a smart contract."[246]

Recital 26 of the draft Data Act confirms that in contracts between a data holder and a consumer as a user of a product or related service generating data, the Unfair Contract Terms Directive applies to ensure that the consumer is not subject to unfair contractual terms.[247] Importantly, through its Article 13, the draft Data Act provides protection against unfair contract terms to micro-, small- or medium-sized enterprises, recognizing that in a data economy characterized by strong asymmetries of power, micro-, small- or medium-sized enterprises might be in as dependent a position as consumers traditionally are vis-à-vis traders. Article 13(5) of the draft Data Act only applies to specific clauses that are "unilaterally imposed" by one contractual party on the other, a much more restrictive test than the Unfair Contract Terms Directive, which refers to those terms that were not

[240] https://www.academia.edu/60233807/Reglementarea_conceptului_de_smart_contracts_%C3%AEn_dreptul_civil_rom%C3%A2n.

[241] European Law Institute, 'ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection' (European Law Institute 2022), 41-42.

[242] Whereas blockchains are generally referred to as being immutable. This terminology has to be qualified. See further https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2940335

[243] Mentioned in the Cypriot national report.

[244] Case C-472/20 *Lombard Pénzügyi és Lízing Zrt. v PN* [2022] ECLI:EU:C:2022:242.

[245] Ibid, paras 57, 60.

[246] Mentioned in the Cypriot national report.

[247] Recital 26 of the draft Data Act ("In contracts between a data holder and a consumer as a user of a product or related service generating data, Directive 93/13/EEC applies to the terms of the contract to ensure that a consumer is not subject to unfair contractual terms. For unfair contractual terms unilaterally imposed on a micro, small or medium-sized enterprise as defined in Article 2 of the Annex to Recommendation 2003/361/EC, this Regulation provides that such unfair terms should not be binding on that enterprise").

"individually negotiated". As a consequence, where a party simply accepts the contract without resistance, Article 13 of the draft Data Act does not apply whereas, pursuant to its Article 3(2), the Unfair Contract Terms Directive does apply. It has been recommended that to mitigate the shortcomings of this formulation, "courts may also use model contract laws as a source of inspiration when applying the general control standard of Article 13(2)".[248]

The Unfair Contract Terms Directive classifies as unfair a non-individually negotiated term if "*contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer*".[249] Any such clauses are not binding on the consumer.[250] This can include terms that compel consumers to share data with third parties.[251] Unfairness control applies irrespective of the format in which a consumer contract is concluded. Indeed, one may argue, that choosing formats such as a smart contract, which at least in their current form, risk being more opaque to consumers than traditional paper contracts, reinforces the need for such protection.

Where a consumer contract contains a term considered to be unfair, that specific clause is not binding on the consumer.[252] The legally binding agreement continues to bind the parties as to the remaining terms if it can exist in isolation from the unfair terms.[253] This implies that smart contracts need to be modifiable. Indeed, a contractual term that *'is not in conformity with the protection consumers are given under the Unfair Terms Directive must be recoded*' in a manner that does not affect the rights and duties of the parties under a previous smart contract.[254] This raises the question of the practical implementation of this requirement where smart contracts are used. Article 30 of the draft Data Act does not require that transactions can be reversed.

Indeed, the technical tamper-resistance of a smart contract's outcome does not entail that the legal relationship that is shaped by the smart contract is or can also be unmodifiable. As the European Law Institute has recently opined, a solution could be a '*follow-up smart contract that would make a previous smart contract 'mute' can change that relationship or express what should have been the content of that relationship in the first place*'.[255]

Thus, also here, model contract terms that provide that in such circumstances, transactions ought to be reversed or their outcome otherwise amended would be helpful. At the same time, interoperability standards would make sure that the smart contract is modifiable in a manner that would be compliant with related requirements of EU consumer protection law.

3.2.6. Termination of contracts and remedies

Challenges for smart legal contracts related to the right of withdrawal

[248] Josef Drexl et al, Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (2022) Max Planck Institute for Innovation & Competition Research Paper No. 22-05, 49.

[249] Article 3(1) of Council Directive 93/13 of 5 April 1993 on unfair terms in consumer contracts (1993) OJ L 95/29.

[250] Article 6(1) of the Unfair Contractual Terms Directive.

[251] This is highlighted by the decisional practice of the Italian competitions and consumer authority. See further, Autorità garante della concorrenza e del mercato, 'WhatsApp fined for 3 million euro for having forced its users to share their personal data with Facebook', 12 May 2017, available at: https://en.agcm.it/en/media/press-releases/2017/5/alias-2380.

[252] Article 6(1) of the Unfair Contractual Terms Directive.

[253] Article 6(1) of the Unfair Contractual Terms Directive.

[254] See further European Law Institute, Council Draft: ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection (2022), 48.

[255] Ibid.

In 23 EEA Member States potential challenges for smart legal contracts were identified by legal experts with regard to specific provisions on the right of withdrawal(**BE, CY, CZ, DE, DK, ES, FI, FR, GR, HR, HU, IE, IS, IT, LT, LU, MT, NL, NO, PL, PT, RO, SK**), whilst in the remaining 7 EEA Member States no challenges by national legal experts were detected in this regard (**AT, BG, EE, LI, LV, SE, SI**).

The right of withdrawal exercised due to force majeure was identified as a challenge to smart contracts by legal experts in 18 EEA Member States (**BG, CY, CZ, EE, ES, FI, FR, HR, HU, IE, IS, IT, LT, MT, NO, PL, RO, SI**).[256]

Legal experts in 12 EEA Member States (**CZ, FI, FR, GR, HU, IT, MT, NL, PL, PT, RO, SK**) pointed out a challenge posed in the area of the right of withdrawal for smart legal contracts is that due to their automatic nature based on blockchain technology, they cannot reflect the depth and diversity of contract law (e.g. if the right of withdrawal is stipulated by law, but it is not integrated into the smart contract), and thus the right of ex-post amendment (for example, in case of an unexpected change in circumstances). To introduce a modification, a new smart legal contract is required, while the original smart legal contract will remain in the system of smart contracts. This would raise doubts about the validity and legal effect of parallelly existing smart legal contracts.

Another challenge brought up by legal experts in two EEA Member States (**ES, FR)** was that the interpretation of the right of withdrawal can create complications in the context of smart contracts, as one might lack expertise to give meaning to the programme code related to conditions triggering the right of withdrawal. Consequently, the correct interpretation of the right of withdrawal may be a challenge to the use of smart contracts in other EEA Member States too.

Furthermore, one of the challenges mentioned by a legal expert from Germany that could pose a challenge to all EEA Member States relates to the prohibition of unlawful interference with possession.[257] Across the EEA Member States, the unauthorised enforcement of contractual rights by technical means of coercion is not allowed. In the German case,[258] a company remotely prevented a car battery from charging, as the company decided to terminate the car renting contract. The court declared that the renter of the car lost the ability to use the rented vehicle, and thus the company caused an unlawful interference with the possession of the renter. Furthermore, in such cases, the reversed burden of proof (from creditor to debtor) would also create problems for smart legal contracts across the EEA Member States as it would undermine the level playing field in the business-consumer relation.

Challenges

In short, the right of withdrawal was harmonised at the EU level, thus the challenges are similar in all EEA Member States. The most important challenge related to the right of withdrawal lies in the immutability of smart contracts, as the automated nature of smart

[256] It should be noted that under Directive 2011/83/EU, this is an EU level requirement on B2C level, and therefore relevant in all Member States. A separate section (3.1.5) focusses on EU consumer law requirements and their relevance in case of smart contracts.

[257] Article 858 of the German Civil Code.

[258] Judgment 20 U 116/20 of 7 October 2021 of the Higher Regional Court of Düsseldorf (Oberlandesgericht Düsseldorf), available at: https://openjur.de/u/2382975.html.

contracts would make the exercise of this right, as well as the incorporation of modifications (e.g., ex-post amendments due to change in circumstances) related to the right of withdrawal difficult. In other words, stepping back from the right of withdrawal or adding new amendments regarding this right could prove to be challenging for the application of smart contracts.

Remedies available for smart legal contracts that are void

All EEA Member States have remedies applicable to smart contracts if they were to be void or declared so by court.[259] Specifically, almost all legal experts from EEA Member States mentioned the option for the reversal of a transaction (a right to *restitutio in integrum*), with 5 exceptions (**CZ, DE, DK, FI, LV**). The second most widely present remedy available in Member States **(**for example, **AT, BG, CY, CZ, DE, DK, EE, FI, GR, HU, IE, IS, LI, LV, MT, NL, NO, PL, SE, SI, SK**) was the right to claim compensation for the damages caused. It should be noted here that in **Sweden** this right can only be exercised in case the damages were caused by threat or fraud. Thirdly, legislation in Estonian[260], Norwegian and Swedish law[261] contains several provisions of possible remedies that would be applicable to smart contracts, such as withholding performance or reduction of price. In addition, the remedy rules are mandatory in several EEA Member States (for example, **AT, BE, DK, HU, IT, LI, LU, LV, NL, RO, SK**). It should be added, that in **Denmark**, mandatory remedy requirements are in place only in the area of consumer protection and effectively mandatory requirements exist only regarding contracts concerning property (both movable and immovable assets). Furthermore, in **Austria** and in **Liechtenstein**, the law prescribes mandatory remedies depending on the legal basis of the contract.

Challenges for smart legal contracts concerning remedy requirements were detected by legal experts in 19 EEA Member States (**AT, CY, CZ, DK, EE, ES, FI, GR, HU, IT, LI, LU, LT, MT, NL, PL, PT, RO, SK**), while none were reported in the remaining 11 EEA Member States (**BE, BG, DE, EL, FR, HR, IE, IS, LV, SE, SI**). Firstly, the immutable and automatic nature of smart contracts was mentioned in 12 EEA Member States as a possible challenge (**AT, CZ, DK, ES, FI, HU, IT, LI, LT, MT, PL, PT**), as reversing executed remedies, as well as amending remedy-related provisions could face hurdles. Secondly, the uncertainty surrounding the identification of the contracting parties was also flagged as a potential challenge (**DK, EE, GR, PL**). For example, in case of **Estonia**, if a performance is defective, a party can accept such a performance (and in parallel may reduce the price) by making a declaration to the other party. However, in case of smart contracts, the identification of the other party might pose a challenge. A third challenge reported by 4 EEA Member States (**CY, PL, PT, SK**) arose from the interpretation of remedy requirements in case of smart contracts, because interpreting more abstract remedy clauses (i.e. clauses including formulations more open to interpretation) could prove to be difficult. In this regard, common law principles and legislation on penal clauses[262] pose a distinct challenge in **Cyprus**, as Cypriot case law considers provisions on extravagant penal clauses non-existent. It is uncertain, if the detection and right interpretation of such clauses would be possible in case of smart contracts Fourthly, the **Netherlands** shared a possible obstacle, which is the inability to undo the contract not due to the nature of smart legal contracts but to the nature

[259] The applicability of remedies on smart contracts is uncertain in Iceland due to lack of legislation and existing case law.
[260] Article 108 to 118 of the Law of Obligations Act.
[261] Sales of Goods Act.
[262] Section 74 of Contract Law (Cap. 149).

of the performance (e.g. transporting service) or by the actual impossibility to undo the contract due to objective circumstances (e.g. the good is destroyed but the payment was already made). Lastly, in **Finland**, identifying the person bearing responsibility for damages in case of a smart legal contract could create challenges (i.e. joint or individual liability of the programmer and the user of a smart legal contract).

Challenges

All EEA Member States have remedies in force. The main challenges in the application of these rules to smart contracts include immutability of smart contracts, identification of parties of a smart contract, as well as the liable party (programmer or users of the contract). Moreover, challenges also stem from the interpretation of remedy requirements.

Restitution rules applicable to smart legal contracts

General restitution rules of civil law would apply to smart legal contracts in all EEA Member States. It should be highlighted that experts in six EEA Member States (**DK, IE, IS, LT, LV, NO)** indicated uncertainty regarding the application of restitution rules on smart legal contracts, due to lack of legislation and/or case law in their respective legal systems. In 11 Member States legal experts indicated that the restitution would mostly be based on the principle of unjust enrichment (**BG, CY, DE, EE, FR, GR, HU, IE, IT, LV, PL**).

In several EEA Member States (e.g., **BE, FR, HU, IT, LU, PT, RO**), the restitution is primarily made in kind (i.e. returning the same or equivalent good to the other party) and if this is not possible, a monetary compensation can be claimed. For example, in **Malta**, in case of defective performance a repair or a replacement (e.g., if a good cannot be repaired) can be sought. If the repair or replacement of the product is either not possible or these would cause the buyer a significant inconvenience, a partial or full refund of the amount paid for the performance can be pursued (within two years). Additionally, in case of **Belgium** and **Luxembourg,** it was indicated that the automatic nature of smart contracts, along with the subject of restitution (e.g. returning a physical object) create challenges for the application of smart legal contracts.

The rules on restitution show similarity in the EEA Member States under examination and thus could apply in a similar way to smart legal contracts in almost all Member States. The following paragraphs will display some Member State exceptions, which show divergence from mainstream rules.

In **Estonia**, three cases[263] exist, where restitution rules do not apply, which would also be applicable to smart contracts. Firstly, when the obligation performed by the transfer is imperfect. Secondly, if the right to demand performance of the obligation has expired by the time of the transfer. And thirdly, in the case of a void transaction, if the restitution would be contradictory to the provision describing the nullity of the transaction.

In **France**, a compensation can be sought for a remaining prejudice even after the restitution has been made.[264]

In the case of **Poland**, it is worth mentioning that the literature on restitution rules discusses cases of contracts concluded electronically. For example, scholars hold that if an order for

[263] Article 1028 of Law of Obligations Act.
[264] Article 1240 of Code Civil.

a payment to be issued in the electronic writ proceedings, it must be effectively served to the defendant along with a copy of the statement of claim. If a copy of the statement of claim (along with the order) is not effectively served to the defendant, a restitution cannot be claimed.

Contract termination rules applicable to smart legal contracts

It should be emphasised that general rules of civil law of EEA Member States related to contract termination would apply to smart contracts (along with rules of private international law).

For example, in Germany, according to private international law, the centre of a legal relationship (i.e. the centre of the vital factual circumstances) is required as a connecting factor to determine the choice of law, if nothing was agreed upon by the contracting parties. In other words, the dominant opinion among German legal scholars[265] is that for smart legal contracts, the relevant contract law is determined by the Rome I Regulation.[266] It should be added, that even if the parties have made a choice of law, the Rome I Regulation still applies. For consumer contracts, the Rome I Regulation limits the free determination of applicable rules, and the place of habitual residence of the consumer is decisive.[267]

Legal experts in certain EEA Member States raised possible challenges (**BG, CZ, IT, PL, SI**) relating to contract termination. In the following paragraphs, the focus is on these EEA Member States.

In **Bulgaria**, the application of the general rule for contract termination is uncertain for smart contracts, as the current legislation requires the creditor to inform the debtor in writing about the contract termination, as well as to provide the debtor with an adequate term for remedying its breach and to request explicitly the return of all transferred assets along with an adequate compensation. Legislative changes would be necessary to ensure that these provisions are practically applicable to smart legal contracts.

In **Czechia**, contract termination rules stipulated by law could pose a challenge for smart legal contracts, if such rules are not coded into a smart legal contract. In such cases, the execution of a smart contract would continue contrary to legal provisions (due to the absence of such provisions from the smart contract) leading to unjust enrichment.[268]

In **Italy**, although the general rules of contract termination would be applicable to smart legal contracts, the act of termination would require a modification of the smart legal contract, which would, as mentioned before, lead to a technical challenge created by the immutability of blockchain technology. Based on scholars' opinion, a termination would be valid in case of smart legal contracts, if the performing party (terminating the smart contract) can rely on remedies in case of non-performance of the other party (e.g. compensation of

[265] Bilski, N., ‚Blockchain-Technologie, Smart Contracts und selbstvollziehende Verträge - Eine Analyse der Chancen und Risiken einer Zukunftstechnologie sowie der Vereinbarkeit der Systemkreise Technik und Recht, Study for the Federal Ministry for Justice and consumer protection', 2019. Available at: https://justice.wifa.uni-leipzig.de/wp-content/uploads/2019/08/JUSTiCE-Juristisches-Gutachten-2019.pdf.

[266] Article 4 (and following) of Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations.

[267] Article 6 of Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations.

[268] Section 1998 of the Czech Civil Code.

damages) and the termination as a result of non-performance attributable to intent or gross negligence is not excluded.[269]

In **Poland**, similarly to Italy, the challenge of immutability of smart legal contracts in the area of contract termination was indicated. The issue raised is that after the parties have made a declaration of will to be bound by the contract in a programming language, it is not possible to return to the state before the conclusion of the contract, without interfering with the smart contract or without applying a new smart contract with the opposite effect. The legislator partially regulated (in the Act on Consumer Rights) situations where performance consists in providing consumers with digital content, unsaved on a tangible medium.[270] However, this provision only covers cases in which the execution of the performance towards the consumer takes place with their express consent, and prior to the deadline for submitting a declaration of the right of withdrawal from the contract.

In **Slovenia**, general rules could be applied, but if the mechanism of the smart legal contract does not give parties the option of terminating the contract under the conditions prescribed by law and the contract is self-executed regardless of the circumstances, then the termination and its consequences should be executed subsequently, off the blockchain. Furthermore, a special area with potential obstacles is the electricity and gas supply sector, due to specific rules on termination of electricity and gas supply contracts. According to Slovenian legislation, the distribution system operator shall not disconnect the electricity of a vulnerable customer or limit their electricity consumption below the amount or power that is strictly necessary under current circumstances (for example, taking existing temperature conditions into consideration).[271] This means that an obstacle could be present in this specific case, as these rules might not resonate well in each case with the automatic nature of smart legal contracts.

Challenges

Contract termination rules would apply in all EEA Member States. The challenges faced here stem from form requirements related to contract termination laid down in Member State legal systems (for example, in Germany, in cases where legislation requires that a contract must be terminated in writing), as well as the immutable nature of smart contracts (i.e. once the act of termination of the smart contract is completed, the return to the state before termination is not possible without creating a new smart contract).

3.2.7. Conclusions

The analysis shows that very few EEA Member States currently have legislation in place that specifically regulate the use of smart contracts. Therefore, the use of smart contracts has to be analysed predominantly based on general national civil law rules applicable to them. First, our analysis revealed that three Member States[272] have passed specific legislation on smart contracts. The definitions of smart contracts in these EEA Member States are similar in that they abstain from a restrictive formulation. Theoretically, this gives enough room for manoeuvre in their application in both domestic and cross-border

[269] Article 1229 of the Italian Civil Code.
[270] Article 38 of the Act on Consumer Rights.
[271] Electricity Supply Act (*Zakon o oskrbi z električno energijo*), No. 172/21 and Gass Supply Act (*Zakon o oskrbi s plini*), No. 204/21 and 121/22.
[272] GR, IT, MT.

contexts. Nevertheless, since these laws are recent and related case law is absent, empirical evidence on their application and their impact is limited. As a consequence, a comparison on the impact of smart contracts legislation between EEA Member States with existing legislation and EEA Member States without existing legislation is challenging. Furthermore, the definitions of smart contracts in Greece, Italy and Malta resonate well with the definition laid down in the draft Data Act, which shows a tendency towards coherence of smart contract definitions.

Second, our analysis revealed that legal experts in EEA Member States with existing smart contract and/or DLT legislation and legal experts in EEA Member States without such legislation indicated challenges in the same proportion (in a wide range of areas, for example the immutable nature of smart contracts, the interpretation of smart contracts, or hurdles posed by form and other essential validity requirements). As the number of EEA Member States with specific legislation on smart contracts is currently low, smart contracts are governed by the general civil and contract law rules, which can have similarities across EEA Member States. As a consequence, the challenges posed to smart contracts are similar in EEA Member States with or without specific legislation on smart contracts. Moreover, as it can be derived from the economic analysis (section 3.1 above), the uptake of smart contracts is limited in practice in all EEA Member States (including in those with specific legislation focusing on smart contracts). Therefore, the practical implications and the impact of specific legislation covering smart contracts is difficult to measure empirically.

In the future, potential EEA Member State legislation could have a negative impact on the internal market, if certain EEA Member States choose divergent regulatory solutions (for example, specific legal rules diverging from general rules). Thus, keeping in mind the possibility of emerging specific legislation and the potential negative impact of divergent regulation remains relevant.

This study has defined obstacles as diverging mandatory measures in an EEA Member State, which have the effect of preventing or hindering fundamental freedoms or distorting competition within the internal market.[273] An obstacle for smart contracts specifically is a diverging mandatory measure (typically civil law rule) that prevents or hinders the uptake and roll-out of smart contracts within the internal market, while challenges are defined as potential obstacles and/or rules that are not easily compatible with the smart contracts technology. Seen through this conceptual lens, national measures at this stage remain challenges due to the missing empirical evidence that national civil law rules in fact do have the effect of preventing or hindering the fundamental freedoms or competition in the internal market. If there is an economically significant uptake of smart contracts in the future, current challenges would, however, become obstacles.

Although no existing obstacles have been documented so far by empirical evidence, also due to the currently very limited use of this technology, existing civil law rules in EEA Member States that smart contracts can currently not meet from a technical perspective (such as those on the validity of smart contracts) may indeed hinder the take-up of smart contracts if and when these are deemed useful from a technical and economic perspective. Indeed, it has been seen that national rules, such as those related to contract formation, are difficult to implement by a smart contract. Thus, not only diverging rules that can

[273] Case C-376/98 – Germany v Parliament and Council (*Tobacco advertisement judgment*).

constitute a challenge for smart contracts but also other rules which are difficult for the smart contracts technology to comply with, which can include also harmonised rules, such as the ones described above.

The identified challenges could become obstacles causing friction within the internal market: this can happen either due to the introduction of mandatory rules in various EEA Member States, or due to an increase in the uptake and application of smart contracts. It should be underlined however, that the transformation of challenges into obstacles (i.e. when a measure is not only potentially, but empirically hinders the use and uptake of smart contracts) currently remains hypothetical based on the evidence gathered in the course of our economic analysis. Therefore, drawing solid conclusions on actual obstacles for the internal market is premature.

Fourth, if greater uptake of smart contracts is experienced in future, national civil law rules may well have a negative impact on the use of this technology in the internal market. Economic operators and consumers in EEA Member States with a legislative environment more friendly to smart contracts would then be in a more advantageous situation compared to economic operators in EEA Member States with more rigid measures. For example, an economic operator that decides to apply smart contracts in their daily business will be able to conduct their business in smart contract friendly environments easily, which could also contribute to creating synergies in these EEA Member States (e.g., an exponential use of smart contracts in other sectors or by other businesses could follow). At the same time, such economic operators aiming to expand their activities to EEA Member States with more inflexible measures would run into obstacles in exercising cross-border smart contract-based economic activities, as well as cut off consumers from receiving smart contract-related goods and/or services. Such a situation would lead to discrepancies in the internal market. What is more, the free movement of goods or services using smart contracts in the internal market would be hampered if smart contracts can be used in one EEA Member State but not another.

Contract law rules, which are equivalent to measures in the framework of this study, could have an impact on the application of smart legal contracts. EEA Member States with legislation in place on contract interpretation and full evidential value showed similarities both in types of rules and types of challenges. In both cases, a major challenge for smart legal contracts stems from the nature of smart contracts, namely that they are formed of code. This makes it difficult to interpret the intention of parties (or other more abstract notions) and to vest smart contracts with full evidential value.

The automatic and immutable nature of smart contracts also poses challenges for EEA Member States as regards ensuring the right of withdrawal (which needs to be ensured in B2C contracts in all Member States in line with the Consumer Rights Directive[274]) and the right to suspension, as certain situations (e.g., force majeure) require precise and adaptable provisions in a smart legal contract. Similarly, these attributes of smart legal contracts would pose challenges for remedies in case of void smart contracts and in case of terminating smart legal contracts. This is at least an issue of lacking legal certainty, as it

[274] 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, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0083.

is presently unclear whether, for example, a second smart legal contract deployed to operationalise the right of withdrawal in relation to a smart legal contract deployed earlier would satisfy existing legal requirements.

In terms of the formation of a contract, as a general rule in all EEA Member States, the principle of freedom of form is established: the parties are free to decide the form of the contract unless there is a requirement of a specific form in the law. Notably, the requirement of a specific form for certain contracts can be challenging for smart legal contracts. Particularly, the requirement of notarial authentication and/or registration with public authorities can pose a challenge, as this cannot be fulfilled by the smart contract itself. In most Member States a contract is deemed formed/created/concluded when the offeror receives the acceptance of the offer. This acceptance can be done verbally, tacitly or through performance in some EEA Member States. According to some EEA Member States' legislation, a contract is concluded simply once the parties' consent is given.

In relation to the formation of a contract, some challenges can arise with regard to the constitutive elements of a contract. Notably, an issue regarding the consent of the parties and its validity or integrity may arise, as the developers are the only ones capable of coding the conditions of the contract. Furthermore, the legal capacity required for entering the contract may not be possible to check in the case of smart legal contracts, as the real identity of the parties involved may not be possible to validate. Finally, the offeror in a smart legal contract may not become aware of the acceptance by the offeree at the same instance the pre-requisites for the execution of the smart legal contract are fulfilled. In addition, the 'lawful consideration' (causa) and/or its moral character may be a challenge to effectively monitor and enforce for smart legal contracts in some cases. Contracts with unlawful or immoral consideration are usually prohibited by law, whereas a smart contract used for illegal purposes would be automatically executed without regard to the nature of the consideration.

In terms of challenges related to the validity of contracts, one challenge that can arise is related to mistakes, as the validity of a contract can be questioned where mistaken information has been given. In addition, the validity of the contracts can be affected if the requirements for the conclusion of the specific type of contract are not met or when the parties of the contract do not have the legal capacity required for the conclusion of the contract, thereby representing a challenge for smart legal contracts.

Due to the global nature of the blockchain, challenges for smart legal contracts may arise also in terms of the choice of applicable law in claims related to cross-border transactions. However, including clauses on the choice of law and jurisdiction for dispute resolution in the smart contract could help to mitigate this uncertainty.

Finally, challenges for smart legal contracts can arise in relation to consumer law rules, as the requirements of the right of withdrawal within 14 days, the information requirements for traders, and the formal requirements for the conclusion of distance contracts may be difficult to fulfil through smart contracts.

Harmonised measures (addressing potential regulatory differences between EEA Member States) could be capable of dismantling future obstacles in the internal market. Existing legislative solutions regulating smart contracts point in this direction: the definition of smart contracts in the draft Data Act allows the flexible application of the technological solution smart contracts are based on and avoids divergences between EEA Member States that have already taken legislative steps. Furthermore, a technical solution (with the right level of interoperability, as well as balanced access to smart contract-related infrastructure for economic operators and consumers alike in the internal market) capable of safeguarding specific legal provisions (i.e. certification) could temper the negative effects of legal obstacles to an insignificant level. In other words, if EEA Member States avoid divergences in smart contract definitions and ensure a universally applicable (i.e. interoperable) and accessible technological solution, then potential obstacles could be minimised, as with smart contracts seen as identical to other types of contracts or transactions from a legal compliance perspective.

Several common challenges were identified (within the specific areas of law analysed above) throughout the EEA Member States, which can be considered in light of the abovementioned discussion on the internal market dimension. These common challenges and the EEA Member States in which they have been noted are set out in the table below.

Table 3: Identified challenges in EEA Member States

Groups of identified challenges	Identified challenge	EEA Member State[275]
The immutability of blockchains	The immutability of the blockchain/smart contracts	AT, BE, BG, CZ, DE, ES, FR, GR, HU, IT, LI, LU, NL, PL, PT, RO, SE, SI
Requirements for B2C contracts	The execution of the right to withdraw from the B2C contract within 14 days, as well as the execution of the right of suspension due to the automatic nature of smart contract	All Member States
	The fulfilment of information requirements in B2C contracts (e.g., the use of the language of code in code-only smart contracts may not fulfil the requirement of the contract terms being stated in a clear and comprehensible manner)	All Member States
Potential differences arising from the full evidential value of documents (e.g., in terms of signatures)	The difficulty to assess the moral or (il)legal character of the object of the contract (causa), as well as the automated execution of the smart contract despite the illegal object[276]	BE, BG, CY, DE, EE, ES, FR, GR, HU, IT, LU, LV, MT, NL, RO, SE, SI
	The legal capacity of the parties to contract	BE, CY, DE, ES, FR, HU, LU, RO, SI[277]
Specific contract forms	The impossibility to use smart contracts where the intervention of a notary or other public authorities is required[278]	AT, BE, BG, CZ, DE, EE, ES, FR, GR, IT, LI, LT, LU, LV MT, NL, PL, PT, RO, SI, SK

[275] EEA Member States included in this column are normally those where the issue was proactively raised by our national legal experts. As a general point, it should be noted that the list of EEA Member States for each challenge is indicative, since the identified challenges are mostly general in their applicability to smart contracts and, therefore, can be relevant for more EEA Member States than those noted.

[276] Although this was not identified as a challenge in Poland and Portugal, it does not necessarily mean that the challenge does not exist there, as it is highly likely that the object of a contract cannot be anything illegal.

[277] Although this was not mentioned in the other national reports, this can be a challenge in all EEA Member States.

[278] Although this was not identified as a challenge in Hungary, it does not necessarily mean that the challenge does not exist there, as notarial authentication and public registration are required for the conclusion of certain contracts (such as contracts for the transfer of property rights over immovable property). The national report for Sweden also did not mention this challenge. However, it differs from Hungary in that the Swedish legislation is rather open in terms of the freedom of form and does not require the use of notaries, and the registration of immovable property, for example, can be done electronically. Therefore, it is unlikely that the Swedish rules on this issue would be a challenge to smart contracts.

Challenges arising from dispute resolution	The difficulty to determine the court competent to adjudicate on claims arising in connection with a given smart contract. However, this challenge can be overcome or its effect can be reduced by including clauses on the choice of law and jurisdiction for dispute resolution in the smart contract. This is relevant also for B2C contracts, where the choice of the adjudication court is not free.	EE, IE, IT, MT, PL, RO
	The identification of the parties to the contract	CY, EE, GR, HU, IE, IT, MT, PL, RO
Counterparty identification and agreement	The assessment of the authenticity and integrity of parties' consent	DE, ES, FR, HU, IT, MT, NL, NO, PT, RO, SI
Clarity of interpretation (also including code only contracts)	The use of some expressions - such as "good faith", "best efforts", "reasonable period" etc – can be a challenge to the interpretation of smart contracts	All Member States
Interpretation of legal terms (including the addition of specific and/or individual provisions)	The overall difficulty in comprehending and interpreting the language of code not only by the parties but also by courts[279]	BE, BG, CY, CZ, DE, DK, FI, FR, GR, HR, HU, IE, IS, IT, LU, LV, MT, NO, PL, RO, SE, SI, SK
	The difficulty to add individual provisions to the smart contract[280]	BG, DE, EE, ES, FR, HU, IT, MT, NL, PL, PT, SI

[279] Although the national reports for Estonia, Netherlands, Portugal and Spain did not mention this challenge, it does not necessarily mean that the challenge does not exist there, as there is a high chance that the issue of understanding and interpreting code language by non-technical professionals exists in all Member States.

[280] Although the national reports for Greece, Romania and Sweden did not mention this challenge, it does not necessarily mean that the challenge does not exist there, as this is intrinsic to smart contracts. In other words, it is a technical issue of smart contracts, not one that relates to the domestic law of a given country.

3.3. Technical feasibility assessment

This section combines the main findings from the legal desk research and creates a path for understanding the feasibility of applying technical solutions to the challenges identified. Section 3.3.1 further draws on three case studies covering smart contract applications implemented by deltaDAO AG, CashOnLedger and Bosch. A feasibility matrix (Annex III) complements this by providing further visual information on the defined challenges and their technical counterparts.

Differences within legal regimes, recognition of smart contracts, definition of smart contracts and how they are used across Member States and within the EEA has led to an equally different set of defined obstacles. At the same time, the availability of technical solutions with respect to the deployment of smart contracts are equally diverse. Different blockchain networks also make use of various programming languages. These are used to create smart contracts for a variety of complex business cases. As such, the jurisdiction where the smart contract will be deployed plays a role in how consumer protection, operational security and other regulations affect the smart contract. For this study, the most commonly occurring challenges have been compiled. Technical feasibility solutions related to the identified challenges will draw wherever possible on the case studies and create a knowledge path connecting the legal desk research, technical feasibility assessment and data governance streams.

Section 3.3 Technical Feasibility Assessment is meant to link both the Comparative Law Analysis under Section 3.2 with the Analysis on personal data management tools based on DLT under Section 3.4. In doing so, Section 3.3 is bridging both identified challenges related to smart contracts and the use of smart contracts in the context of the Data Act. Section 3.3.1 follow a specific chronology drawing wherever possible on both streams of analysis, including when discussing the case study findings. The same chronology is highlighted in the Feasibility Matrix (Annex III) further referencing the case studies. Section 3.3.2 further assesses a suite of Techno-Economic solutions drawing both from those enumerated within the Data Act alongside other technical abstractions employed in the utilization of smart contracts under different market conditions. The impact of these Techno-Economic solutions is appraised, both against the Data Act and in the area of public permissionless blockchains.

The most identified challenges in the comparative law analysis were:

- Counterparty identification and agreement.
- Specific contract forms.
- Clarity of interpretation (also including code only contracts).
- Challenges arising from court/dispute resolution.
- Interpretation of legal terms (including the addition of specific and/or individual provisions).
- Immutability of blockchains.
- Potential differences arising from the full evidential value of documents (e.g. in terms of signatures).

Technical feasibility solutions under investigation include:

- Programming languages and available methods.
- Compliance with existing consumer protection at the code level.

- Reverse transaction features.
- Terminability in smart contract design.
- Court/dispute resolution.
- Counterparty identification and smart contract-based liability assignment.
- ‘Embedded supervision’ in ‘permissioned’ DLT environments leveraging on-chain. Data.

3.3.1. Technical Feasibility

The following section examines the identified challenges and relates them to technical feasibility outcomes at the level of the smart contract through three use cases. This will be done to see how the use cases operate inside a given jurisdiction and according to business constraints.

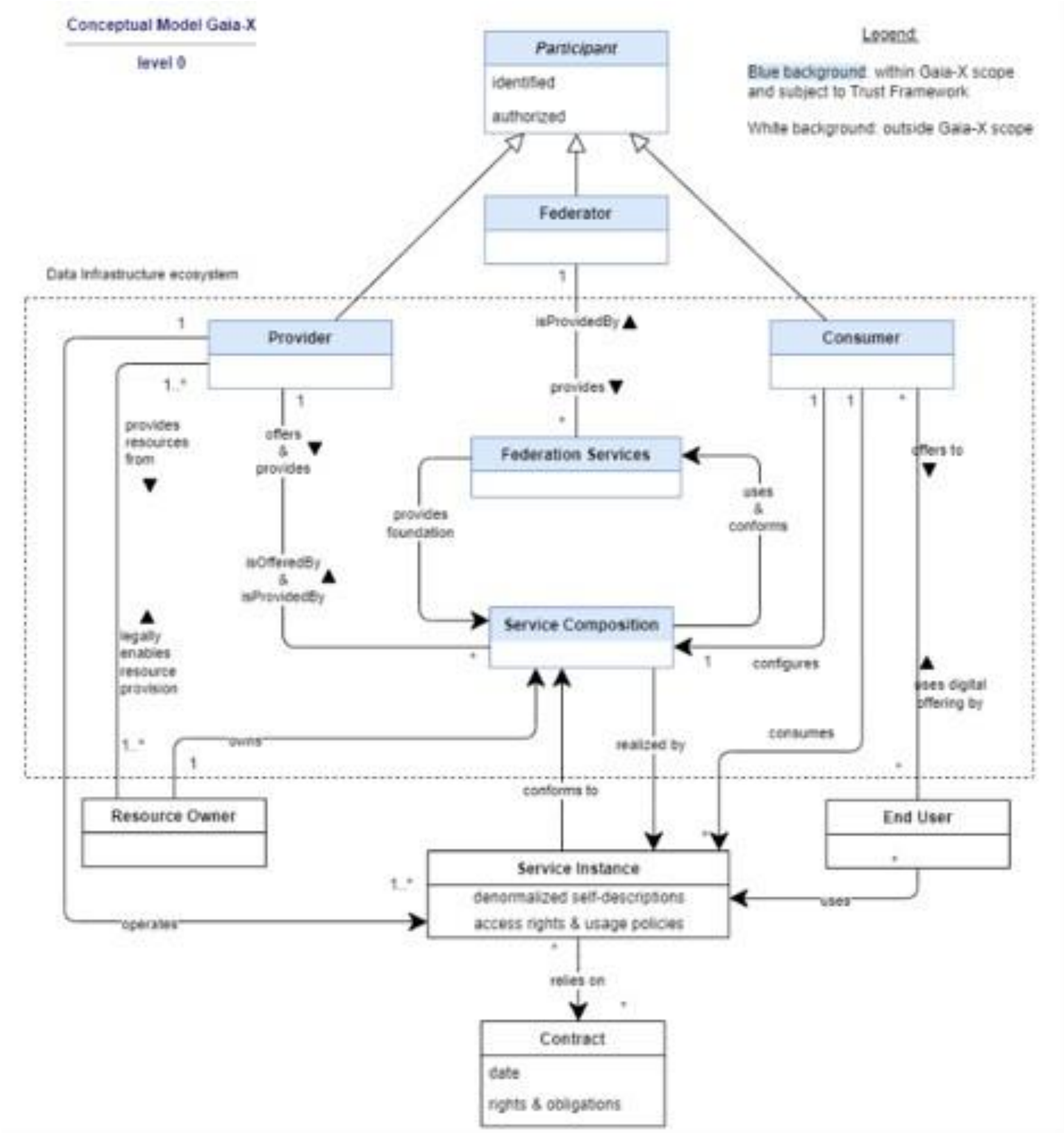
A. Case study technical background

1. deltaDAO AG and the Gaia-X Ecosystem Framework

DeltaDAO AG enables the use of data spaces as a service while maintaining privacy and preserving data exchange. This is achieved within the Gaia-X framework. Broadly, the framework is a system where publishing, discovering, selecting and consuming data service offerings is achieved through portals that provide a user-interface. This allows for interaction with core federation service functions. Portal users can leverage machine learning (ML) algorithms, artificial intelligence (AI) services and federated analysis that allow them to source valuable information from data offerings, or to offer access to their own sensitive data – without risking exposure to unmitigated third-party or compliance risks. Within Gaia-X, deltaDAO has created their minimum viable product (MVP). It represents a data access mechanism called Compute-to-data (CtD). CtD lets data owners to grant compute access to their data without needing to create copies in other environments they do not control. The data itself can remain with the data owner in a secured environment to minimize the risk of data leaks.

The technology aims to be use-case agnostic and dependent on the regulations of different domains. It has an identity layer that is based on the Gaia-X Trust Framework, developed under eIDAS rules for Know-Your Business (KYB). The Gaia-X Architecture enables data - infrastructure ecosystems using the elements explained in the Gaia-X Operational Model and Federation Services together with the Gaia-X Trust Framework. At a technical level, Gaia-X seeks to jointly address data and infrastructure perspectives. The Gaia-X Ecosystem is populated by individual ecosystems that use the Gaia-X architecture and jointly conform to Gaia-X requirements. Participants in Gaia-X ecosystems can take the form of both Consumers as well as Providers.

Figure 3: Gaia-X high-level conceptual framework

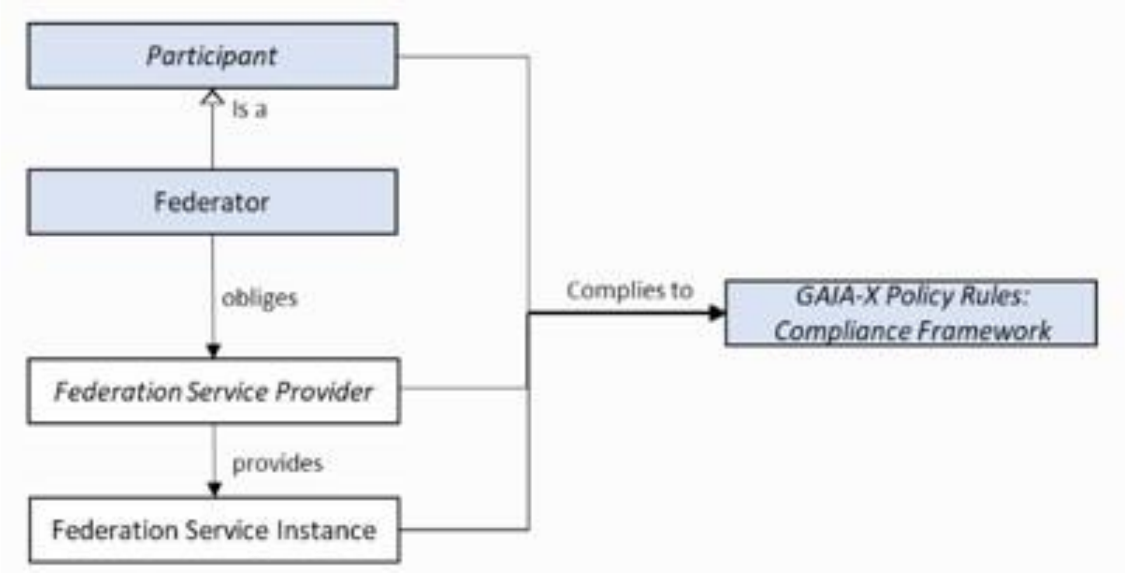


Source: Gaia-X overview level 0

Federated Catalogues are designed to host ecosystem participants. Federations within Gaia-X promote equal, horizontal participation across a range of potential services based on a common set of rules. Services within Federated Catalogues can include technical infrastructure for different use cases, which allows data exchange and data services based on a common data standard. This also allows for software interoperability. Common governance includes the Policy Rules, which are statements of objectives, rules, practices or regulations governing the activities of Participants within the ecosystem and the Trust Framework.[281]

The Gaia-X framework has two main components: Federation Services and Contracting Services.[282]

Figure 4: Gaia-X Federation Services process flow


Participant
Is a
Federator
obliges
Federation Service Provider
provides
Federation Service Instance
Complies to
GAIA-X Policy Rules: Compliance Framework

Source: Gaia-X Federation Services

Building around uniform standards, specifications, rules and policies, Gaia-X is further aligned with NIST Cloud Federation Reference Architecture:[283]

- No single ownership in the context of security and collaboration.
- Gaia-X Association Participants jointly agree on principles of common goals and governance.
- Participants have the option of making their Resources selectively discoverable and accessible to other Participants in compliance with Gaia-X.
- Restricted discovery and information disclosure is available to Providers, albeit at the risk of losing compliance.

2. CashOnLedger (Asset-as-a-Service tokenization model)

CashOnLedger is a Cologne-based start-up that provides a software solution to enable Internet of Things (IoT) payments. This is done through a cloud-based infrastructure where CashOnLedger connects directly to the customer database to obtain relevant billing data. This data is then drafted into legally compliant invoices and the payment claims are settled through connection with participating banks. The CashOnLedger business case is optimized for usage-based business models, so called 'asset-as-a-service' models that can

[281] https://gaia-x.gitlab.io/technical-committee/architecture-document/ecosystem/.
[282] https://gaia-x.gitlab.io/technical-committee/architecture-document/federation_service/#fn:25.
[283] Bohn, R. B., Lee, C. A., & Michel, M. (2020). The NIST Cloud Federation Reference Architecture: Special Publication (NIST SP) - 500-332. NIST Pubs. Available at: https://doi.org/10.6028/NIST.SP.500-332.

be applied in different industries including mobility, logistics and engineering. The business case presupposes a form of digital programmable money that enables value transfer through closed-loop data cycles. In turn, CashOnLedger uses granular data inputs via telemetric sensors to optimize its pay-per-use strategy, based on the time for which an asset is used and the price, determined by the type and value of the asset. The use of blockchain technology enables the asset to be tokenized. Further, DLT infrastructure allows for asset transparency, enabling platform microservices tied to the asset (e.g. insurance) and the creation of automated revenue streams and payments.

3. Bosch (moveID)

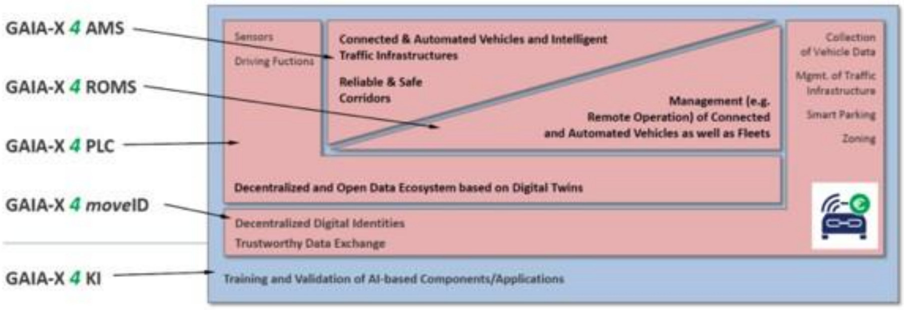
Bosch GmbH is the consortium lead for the moveID project under the Gaia-X 4 Future Mobility umbrella – located in the mobility domain of the German Gaia-X Hub. Working also under the direction of the German Federal Chancellery (*Bundeskanzlerarmt)*, Gaia-X 4 and moveID specifically focus on future mobility applications with high product proximity. Such systems exhibit a high concentration need for data-based networking along the value chain between manufacturers, suppliers, service providers and users.

At a high level, the focus of Gaia-X 4 and moveID is on "non-discriminatory access to digital services in a closely networked, European infrastructure with preservation of autonomy with regard to private data and improvement of security and trustworthiness in a future Internet of Things (IoT)."[284]

In practice, Bosch is concentrated on the development of use-cases related to traffic, such as car-to-car communication, charging, parking and autonomous driving. Examples include finding solutions for, among others, questions related to the availability of vacant parking spots in a city, the availability of unused charging stations and vehicles paying for parking spots or tolls.

To achieve this, the use of decentralized and platform independent technologies including distributed ledgers, self-sovereign identity (SSI) and decentralized data marketplaces are being studied at scale in close work with other consortia partners.

Figure 5: Gaia-X 4 moveID[285]


GAIA-X 4 AMS
GAIA-X 4 ROMS
GAIA-X 4 PLC
GAIA-X 4 moveID
GAIA-X 4 KI
Sensors
Driving Fuctions
Connected & Automated Vehicles and Intelligent Traffic Infrastructures
Reliable & Safe Corridors
Management (e.g. Remote Operation) of Connected and Automated Vehicles as well as Fleets
Collection of Vehicle Data
Mgmt. of Traffic Infrastructure
Smart Parking
Zoning
Decentralized and Open Data Ecosystem based on Digital Twins
Decentralized Digital Identities
Trustworthy Data Exchange
Training and Validation of AI-based Components/Applications

Source: Gaia-X 4

[284] An introduction to moveID is available at: https://moveid.org/2022/08/16/introduction-of-gaia-x-4moveid/

[285] List of Gaia-X 4 moveID industry partners: 51 nodes GmbH; Airbus Defence and Space GmbH; Atos Information Technology GmbH; BigChainDB; Chainstep GmbH; Continental Automotive Technologies GmbH; Datarella GmbH; DENSO AUTOMOTIVE Deutschland GmbHGerman Aerospace Center: Institute for AI Security; ecsec GmbH; Fetch.AI Research & Development GmbH; Saarland University of Applied Sciences.

B. Programming languages and available methods

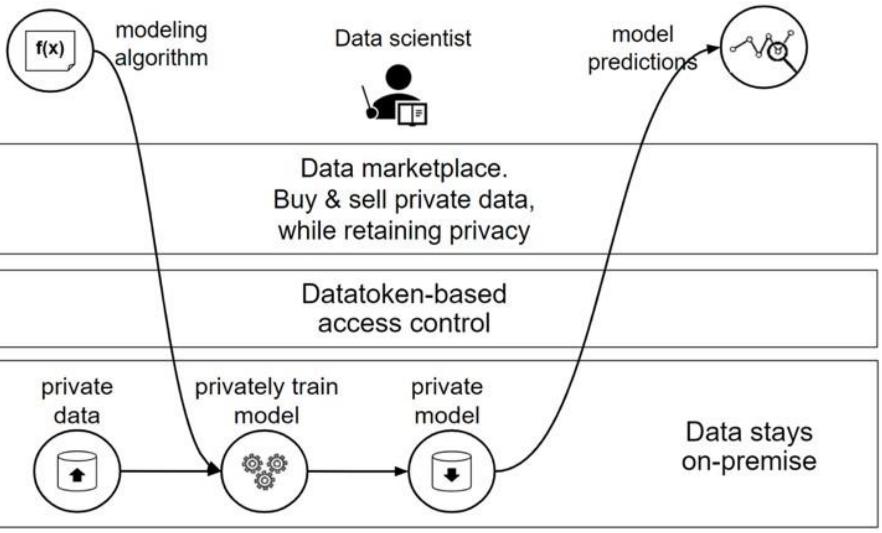
The deltaDAO AG operating model inside Gaia-X is built using the blockchain architecture of Ocean Protocol. Ocean Protocol is a blockchain that lets users transact with their own data as an asset inside data marketplaces. These data assets are coded as both Non-Fungible Tokens (NFTs) and data tokens. The data NFTs use the ERC721 token standard, which is the NFT token standard on the Ethereum blockchain. Data NFTs can be thought of as foundational intellectual property (IP) not unlike a master tape in music. Data tokens are fungible and use the common ERC20 token standard. The possession of one data token for any given data service allows access to that service much like a license against the base IP.

In this context, deltaDAO AG's data access mechanism, Compute-to-Data (CtD), lets data owners provide segregated compute access to their data. This is done in a way that lets data owners retain their data ownership while providing access for it in a marketplace with clearly defined rules and operating procedures that are designed to enable GDPR compliance. Compute-to-Data can make up different typologies.[286] The typologies outlined below assume adjacent model training next to the data exists:

- **Federated learning:** compute operating adjacent to the model is not for training purposes but for another purpose. Example: Person A downloads a trained model, and it leaves Person B. This happens if Person B believes the model exhibits a low-level risk of leaking personally identifiable information (PII), as is the case in linear models or smaller neural networks. Person A can then learn a model across multiple data silos.
- **Aggregating function:** operates beside the data (e.g., an average or median) making CtD useful for certain business intelligence (BI) use cases and more complex artificial intelligence (AI) use cases.
- **Federated analytics**: an aggregation function is computed along multiple data silos.
- **Decoupled hashing:** a hash gets computed for input variable and input value combinations of Person B's data. The compute operates adjacent to the data. Hashing will anonymize the data and Person A then downloads the hashed data to train the model client-side.
- **Differential privacy:** Person B has sufficient random noise added to their dataset for it to qualify as anonymized. Person A then downloads the partly randomized data and trains the model client side.

[286] Trent McConaghy, "NFTs & IP 3: Combining ERC721 & ERC20", Ocean Protocol Blog, Jun. 5, 2021, available at: https://blog.oceanprotocol.com/nfts-ip-3-combining-erc721-erc20-b69ea659115e.

Figure 6: Ocean Protocol Compute-to-Data model



Source: Ocean Protocol Compute-to-Data

Ocean Protocol, and by default deltaDAO, both operate on the Ethereum main network. This includes other Ethereum Virtual Machine (EVM) networks, such as Binance Smart Chain (BSC), Moonriver, Energy Web Chain (EWC) and Polygon. Polygon is the chosen network that operates deltaDAO. It supports different programming languages such as Solidity, Golang and Vyper. The main programming language of the three used by Ocean Protocol is Solidity. The cloud architecture supports Microsoft Azure and Amazon Web Services (AWS), as well as EU public cloud providers such as PlusServer and the Sovereign Cloud Stack (SCS). SCS is the development operations (devops) stack that works on top of the public cloud to support the Gaia-X Federation Services (GXFS).

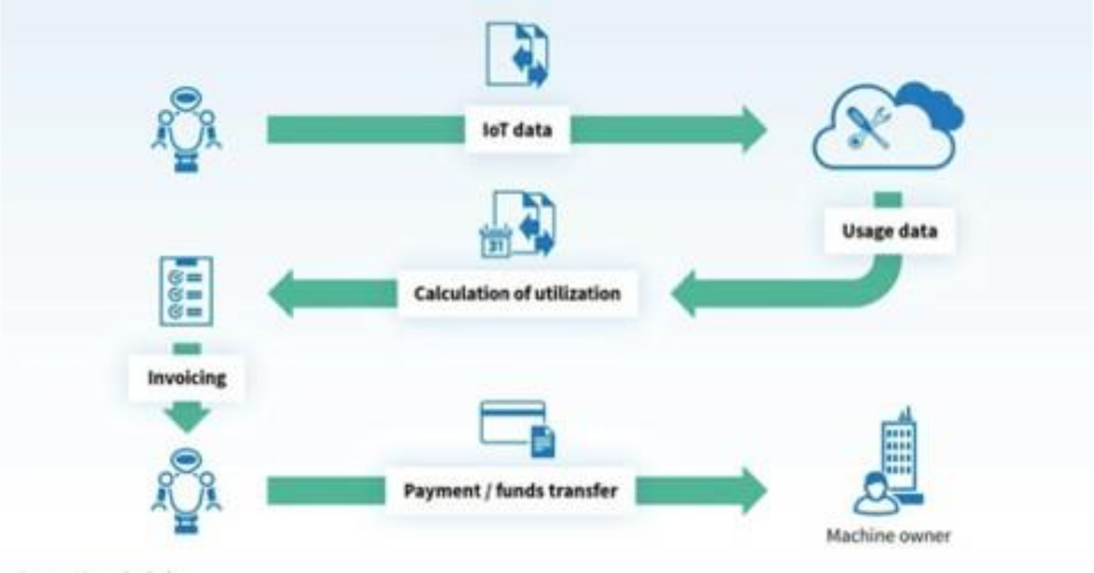
Unlike deltaDAO, around 90% of the solution on CashOnLedger is deployed via Microsoft Azure or other cloud services such as Amazon Web Services (AWS) or Google Cloud Platform (GCP). Only around 10% of the service is deployed on a DLT network. CashOnLedger had initially tried to leverage the Corda blockchain[287] but ended up switching to Quorum[288] because it offered a unified data source.

In the case study, CashOnLedger has partnered with Austrian Tractor Manufacturer Lindner to create full transparency around the usage of Lindner's tractors. Telemetric units retrofitted onto the commercial vehicles collect sensor signals and this usage data is transmitted to CashOnLedger. Once sent, the data records are cryptographically signed, recorded and sorted according to a desired billing model. In the case of Lindner this is optimized for usage type and hours used to draft a receivable and daily invoice. In parallel, this invoice gets transferred to Lindner's own enterprise resource planning (ERP) system.

[287] R3 Corda is a permissioned peer-to-peer distributed ledger technology operationalised for scalable and regulatory compliant development, available at: https://corda.net

[288] Quorum is an Ethereum-based enterprise level blockchain network which supports the programming languages Java and Kotin as well as Solidity for smart contracts, available at: https://consensys.net/quorum/

Figure 7: Asset-as-a-service model based on IoT data



Source: CashOnLedger

Case study interviews have also shown that Bosch is blockchain agnostic with no specific focus on a single blockchain network or programming interface within moveID. The rationale being that currently it is difficult to say what 'winning technology' will exist in the future. moveID is building services around cross-chain communication for a multi-chain future; assuming more than one competing blockchain network at scale long-term. Some of the key blockchain networks mentioned under moveID include Polygon, Polkadot and Cosmos. For each blockchain network, the below table illustrates the main programming languages.

Table 4: Key blockchain networks under moveID

Blockchain Network	Main Programming Languages
Polygon	Solidity, Golang, Vyper
Polkadot	Rust, JavaScript, !ink (for smart contracts)
Cosmos	Ethermint, SecureEcmaScript (SES) for smart contracts, Pact

The moveID consortium is also exploring the full spectrum use of Zero-Knowledge Proof (ZKP) cryptography. There is a separate work package that deals solely with blockchain interoperability issues. At this stage, Bosch is more concerned with focusing on the applicability of each use case to better understand what type of decentralisation technology should be playing a major role. For common characteristics, it is clearer which technologies are to be used. For more specific characteristics, there is a need to first analyse what they entail in terms of specific use-cases/applications and only afterwards to decide what should and should not be used.

Bosch also has specific packages for the decentralisation of data storage and communication which involves possibilities related to the InterPlanetary File System (IPFS).

All three case studies employ a variety of different programming languages and available methods. The common denominator among them is that the Ethereum public blockchain and its secondary layer scaling solutions (e.g. Polygon) are used the most. This makes Solidity the smart contract language most commonly in use. deltaDAO and Bosch are the most interoperable, building solutions under the Gaia-X umbrella that aim to provide complementary use-cases also for decentralized identity and data usage/service agreements. The three case studies also differ in the overall percentage of distributed ledger technology employed and the percentage that is left to various cloud infrastructure providers. This may be associated with current database scalability issues and relative costs.

C. Counterparty identification and agreement

Determining liability for participating users of smart contracts was identified as a commonly cited area of friction. How a challenge might arise from who is behind the screen instantiating a smart contract transaction or whether an individual has the legal capacity to engage in the transaction was another concern. For instance, one can imagine a case where a minor wishing to engage in age restrictive online activity tries to make use of a platform that offers smart contracts. Another example is the use of smart contracts in a situation that requires determining that the consent of parties entering into a contract is genuine.

Counterparty identification is a core principle of the deltaDAO operating model and by extension the Gaia-X framework. It is under the Gaia-X Trust Framework where the rules determining the baseline for acceptance into the Gaia-X ecosystem are provided. The Trust Framework operationalizes requirements as defined by Gaia-X. The scope of the Trust Framework applies to all Gaia-X Self Descriptions:

- All participants, including Consumers, Federators and Providers.
- Service Offering.
- Resource.

The Trust Framework has four types of rules:[289]

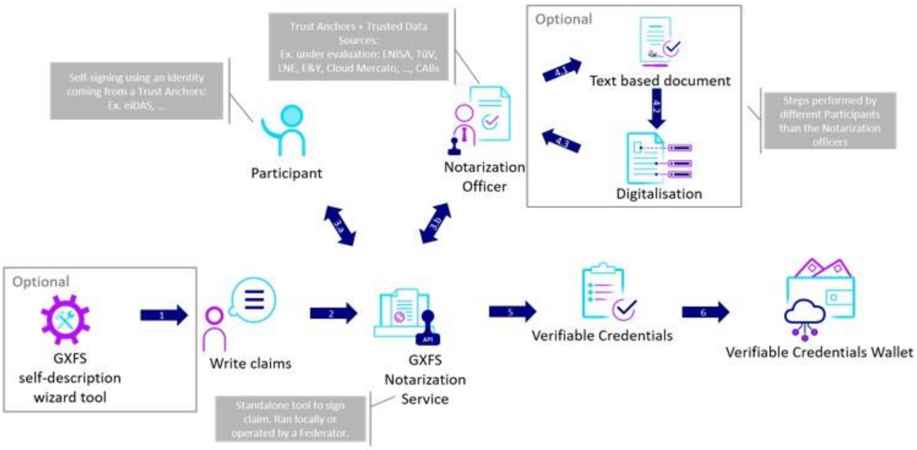
- Serialization format and syntax.
- Cryptographic signature validation and validation of the keypair associated identity.
- Attribute value consistency.
- Attribute veracity verification.

Gaia-X Self-Descriptions comprise machine-readable text which is cryptographically signed and follows the Linked Data principles[290] used to describe attributes. The attribute format is created by using JSON files and human-readable text to store and transmit data objects. The network is divided into different types of participants; however, the participant must be a legal or natural person as defined by law. In this way, determining if a participating user has the legal capacity to enter into a transaction or engage in the network is framed at the beginning of the onboarding procedure. Issuers can create a Gaia X verifiable credential:

[289] https://gaia-x.gitlab.io/policy-rules-committee/trust-framework/#fn:linkeddata.

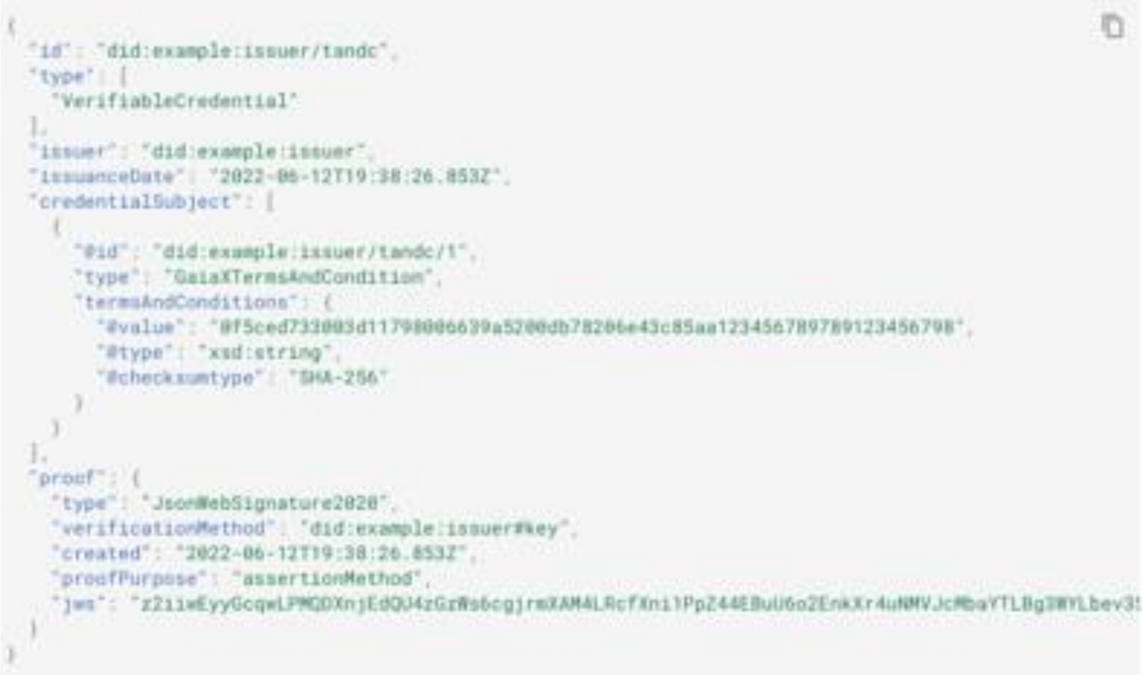
[290] https://www.w3.org/standards/semanticweb/data Linked Data Principles are a type of semantic web standard developed by the Worldwide Web Consortium (W3C). These standards create a structure for making simple statements about resource that allow machines to interpret existing relationships.

Figure 8: Gaia-X Self-Description Creation


Self-signing using an Identity coming from a Trust Anchors: Ex. eIDAS, ...
Trust Anchors + Trusted Data Sources:
Ex. under evaluation: ENISA, TüV, LNE, E&Y, Cloud Mercato, ..., CABs
Optional
Text based document
4.1
4.2
4.3
Digitalisation
Steps performed by different Participants than the Notarization officers
Participant
Notarization Officer
3.a
3.b
Optional
GXFS self-description wizard tool
1
Write claims
2
API
GXFS Notarization Service
Standalone tool to sign claim. Ran locally or operated by a Federator.
5
Verifiable Credentials
6
Verifiable Credentials Wallet

Source: Gaia-X collecting signed claims

Figure 9: JSONPath for Verfiable Credentials



```
{
  "id": "did:example:issuer/tandc",
  "type": [
    "VerifiableCredential"
  ],
  "issuer": "did:example:issuer",
  "issuanceDate": "2022-06-12T19:38:26.853Z",
  "credentialSubject": [
    {
      "@id": "did:example:issuer/tandc/1",
      "type": "GaiaXTermsAndCondition",
      "termsAndConditions": {
        "@value": "0f5ced733003d1179800639a5200db78206e43c85aa123456789789123456798",
        "@type": "xsd:string",
        "@checksumtype": "SHA-256"
      }
    }
  ],
  "proof": {
    "type": "JsonWebSignature2020",
    "verificationMethod": "did:example:issuer#key",
    "created": "2022-06-12T19:38:26.853Z",
    "proofPurpose": "assertionMethod",
    "jws": "z2iiwEyyGcqwLPMQDXnjEdQU4zGzWs6cgjrmXAM4LRcfXni1PpZ44EBuU6o2EnkXr4uNMVJcMbaYTLBg3WYLbev3
  }
}
```

Source: Gaia-X Trust Framework

Table 5: Gaia-X legal person attributes

Attribute	Cardinality	Trust Anchor	Other
registrationNumber	1	registrationNumberIssuer	Country registration number identifying one specific entity.
headquartersAddress.countryCode	1	State	Physical location of headquarters in ISO

			3166-2 alpha2, alpha-3 or numeric format.
legalAddress.countryCode	1	State	Physical location of legal registration in ISO 3166-2 alpha2, alpha-3 or numeric format.
parentOrganization[]	0..*	State	A list of direct participant that this entity is a suborganization of, if any.
subOrganization[]	0..*	State	A list of direct participant with a legal mandate on this entity, e.g., as a subsidiary.

Source: Gaia-X Trust Anchors

Registration numbers used in the validation process must also come from an accredited source. Local registration numbers must correspond to the state issued company number. Within the EEA, the European Unique Identifier (EUID) for those businesses in Iceland, Liechtenstein and Norway applies, alongside those registered in the Business Registers Interconnection System (BRIS).

A corresponding link is created, bringing the user to the Gaia-X Ecosystem Terms and Conditions which must be accepted before continuing:

"*The PARTICIPANT signing the Self-Description agrees as follows:*

- to update its descriptions about any changes, be it technical, organizational, or legal - especially but not limited to contractual in regards to the indicated attributes present in the descriptions.

The keypair used to sign Verifiable Credentials will be revoked where Gaia-X Association becomes aware of any inaccurate statements in regards to the claims which result in a non-compliance with the Trust Framework and policy rules defined in the Policy Rules and Labelling Document (PRLD)."[291]

The Gaia-X framework is still undergoing development and different ecosystem use-cases are being trialled with participants. There is ongoing work to improve the validation process for natural persons including a current project exploring how to validate whether a remote interaction is done by a natural person. The corresponding conceptual framework for this validation process as outlined by Gaia-X is described below:

- WebAuth with FIDO2 dongles.
- An ongoing demo with Yubikey.
- Android applications which use the Google Play Integrity API and a nonce given by the verifier. The returned value of IntegrityTokenResponse.token() must be shared with the Verifier.
- Allowing Push notifications to an application for any workload remote attestation that is supported by TPM2.0 modules.

[291] https://gaia-x.gitlab.io/policy-rules-committee/trust-framework/participant/.

For Verifiable Credentials issued under the Trust Framework to be valid, and therefore allowing the users to engage within different ecosystems, they need to be verified by Trust Anchors (e.g. European Blockchain Services Infrastructure (EBSI) API)[292]. The Trust Anchors underscore all claims by Participants. Through processing these claims they validate trust and elevate the claim beyond the level of a self-declaration. All key-pairs that are used to sign claims need to incorporate at least one of the listed Trust Anchors in their certificate chain to remain compliant with the Gaia-X Trust Framework. The list of valid Trust Anchors is always accessible via the Gaia-X registry.

Table 6: Trust Anchor qualified issuers

Value	Definition
State	The Trust Service Providers (TSP) must be a state validated identity issuer or an EV SSL issuer. - For participant, if the legalAddress.country is in the EEA then valid state identity issuers fall under eIDAS. Gaia-X Association can also serve as a valid TSP for Gaia-X Association members.
eIDAS	Issuers of Qualified Certificates for Electronic Signature as defined in Regulation (EU) No 910/2014.
EV SSL	Extended Validation (EV) Secure Sockets Layer (SSL) certificate issuers are considered to be a temporarily valid TSP.
registrationNumberIssuer	Under the pilot phase, the Gaia-X association self-nominated as a valid Trust Anchor.

Source: Gaia-X Trust Anchors

The exchange of services and service usage transactions are traceable with mandatory applied monitoring and logging. The principle of self-determination also allows Providers to freely choose to apply no usage policies at all. Exchange Services under Gaia-X have different functionality based on before, during or after the transaction. As outlined in the Gaia-X conceptual model in A.1., Service Instances can exist outside the scope of Gaia-X. Therefore, the framework which takes place before the transaction (including drafting any usage policies) is not directly in scope. However, end-users can rely on a given Service Offering on a contractual basis because the contract still presents the legal foundation for Service Instances and their specified policies.

Resource owners, which also exist outside the direct Framework still legally enable resource provision and maintain ownership rights to those resources. Providers are the only ones able to realize both a Service Offering and Service Instance. This does not require further modelling of ownership rights by another legal holder. End-users use service offerings of a consumer that are enabled by Gaia-X. The End-user uses the Service Instances containing self-descriptions and policies.

Agreeing to the contract and to the terms underlying the deployment of the data first begins outside the scope of the Gaia-X Framework and is integrated thereafter. Section A.1. outlined that the backbone of the Gaia-X framework are so-called Federation and Contracting Services. Data Exchange Services make up the core of the contracting services.

[292] https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure

This is followed by a data usage agreement which comprises the associated terms and conditions for the data. In cases where there is a data license attached to the data, the co-signed data usage agreement takes the form of a legal usage agreement. It references explicit license rights determined by the data licensor. The signed data usage agreement is notarized by a Trusted Consent Authority.

The Federated Data Catalogue comprises the list of all data products that have an affixed self-description. Each data contract has a corresponding license that defines its usage policy, including additional information like billing and service level. The data contract comprises a data usage contract template. Prior to any data product use, the data consumer and provider negotiate a data contract. For all strings of licensed data in the data product, the data contract must also include explicit consent to use which is signed by the data licensor. That includes all data usage consent as required under GDPR.

Where deltaDAO and the Gaia-X Framework employ novel Self Descriptions and a Trust Anchor system to identify ecosystem participants, traditional contracts at law govern the terms and conditions of contracting parties that enter into an agreement that makes use of CashOnLedger services at the infrastructure level. The identities, and KYC/KYB information of these parties is known and established from the outset. Transaction data executed through smart contracts further traces relevant actors and asset information on-chain through the node infrastructure and into the ERP and accounting systems of participating parties. In the case of Bosch, the primary challenge for counterparty identification and consent is not so much a challenge of the smart contract as it is of the legal regime as such. The future use cases being explored under moveID presuppose that self-attesting machine identities can interact autonomously, share data, make payments, have credentials and more importantly, that those credentials can be stored in a wallet.

The eIDAS framework under Article 24 allows legal or natural persons to obtain a certificate in a Registration Entity through both synchronous and asynchronous remote video identification. However, neither legal recognition for machines under the current eIDAS framework, nor the proposed amendments under eIDAS 2.0 consider machine IDs as directly in scope. Smart contract execution to optimize payments and data flows between machines would require further legal clarification at EU law.[293]

Bosch has stated that they are currently not focusing on machine-to-machine payments but that this is in scope for future research. As this would require also the provision of un-hosted wallets to machines for the purpose of settling micro-transactions potentially in cryptocurrency, there are questions related to the Markets in Crypto Assets Regulation (MiCA) which may need to be addressed.

Outside of any formal legal clarification for machines, the division of labour under moveID is currently divided into three building blocks:

[293] However, such a framework already has a potential grounding under eIDAS 1 and 2. In brief:
The possibility to introduce decentralized identities also including SSI through the eIDAS Bridge (an EU solution to bridge the centralized approach of eIDAS1 referenced government eID and qualified trust services)
Article 13 eIDAS introduces liability for qualified trust service providers (QTSP). Given that Article 13 remains unchanged under the proposal for eIDAS 2.0 this could also apply to QTSPs, and may imply a public/private permissioned DLT network to ensure there always exists a provider operating and providing such network.

- **Agents:** software agents act on behalf of their owners to achieve both goals and economic activity. These may include vehicles, electric scooters or bikes, parking spaces, charging stations and road tolls.
- **Blockchain:** provides scalable infrastructure to support ecosystem growth.
- **Data oracles:** agent-based oracles which aggregate information about the world using sensors and APIs. These include traffic lights, weather and traffic sensors, IoT devices, APIs and people.

In summary, counterparty identification and consent ranges across the case studies. Where deltaDAO uses innovative attestation methods such as W3C Verifiable Credentials alongside standard contracts, CashOnLedger relies more standard contracts and usage agreements. Through the W3C verifiable credentials, the Gaia-X Trust Framework has created a robust use case for decentralised identity solutions. The addition of Compute-to-Data further underscores this approach. Bosch, like deltaDAO is also building on decentralised identity within the moveID consortia, but in the field of the future of autonomous mobility. The future attestation of machine identities is not defined in national or European law and poses an operational challenge for moveID. Where the Gaia-X participants are seeking to merge attestation through trusted API frameworks, CashOnLedger as an infrastructure provider connecting two parties, can simply rely on written form contracts between itself and Lindner Tractors. It remains that identifying parties to a transaction with the use of smart contracts relies most successfully on a combination of written form contracts and code-base. At least with respect to the current status quo.

D. Specific contract forms

It was identified in the comparative law analysis that instances which require notarial addendum or otherwise registration at a public registry (e.g., in the case of immovable or real property) include formalities which a smart contract cannot satisfy on its own. Furthermore, a code-only smart contract would not be sufficient to consider it as written form. Under Article 8(1) of the CRD[294], information must also be available in a natural language version corresponding to the code. Further, Article 28(9) GDPR stipulates that ‘suitable documentation’ shall be in writing, including electronic form.

Contracts are not directly within scope of the Gaia-X framework but provide a parallel legal grounding for any in-scope activities between consenting users. deltaDAO and Gaia-X solve this duality in two ways: (i) the data usage template and (ii) the data contract which is designed as a Ricardian contract. In the Gaia-X Policies, under General Provisions, it states that ‘the provider shall offer the ability to establish a contract under Union or EU/EEA/member state law and specifically address GDPR requirements.[295]

The contract model template in Figure 8 shows how non-computable contracts in conjunction with Service Offerings aim to satisfy the criteria under GDPR. Because this is a combination of written form and codebase, where notarial addendum is required, parties have the optionality to do so. There is also an effort within the Gaia-X Association to establish templates and facilitate ‘contracts as a service’ to bridge the technical and

[294] 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:32011L0083.
[295] https://gaia-x.eu/wp-content/uploads/2022/05/Gaia-X_Policy-Rules_Document_v22.04_Final.pdf.

analogue domains at law. These principles are meant to inform Participants when negotiating the baseline for their contractual relationship:

"Contracts are the basis for business relationships.

Whereas a licensor has rights with respect to a resource and is willing to (sub-)license such rights by a defined set of conditions.

Whereas a licensee would like to get license rights with respect to a resource by a defined set of conditions.

Licensor and licensee agree on it in form of a contract.

Every role of the Gaia-X Conceptual Model as well as of operational model can be seen as legal persons and therefore may have a role as a licensor or licensee or both.

In traditional centralized driven ecosystems, the platform provider, which is very often the ecosystem owner, defines the contractual framework and participants need to accept without any possibility for negotiation.

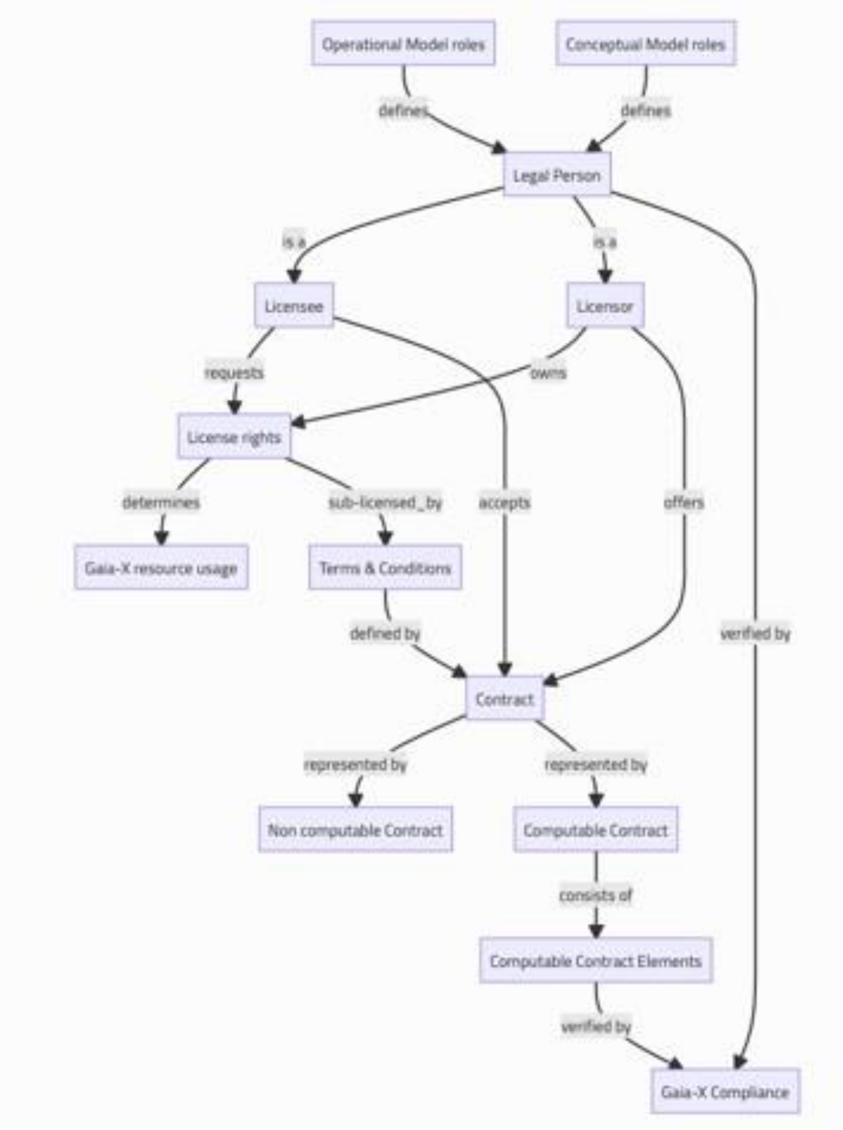
In distributed and federated ecosystems individual contracting becomes much more important to support individual content of contractual relations, e.g., individual sets of conditions.

The ability to negotiate contracts is key for sovereign participation. The ability to observe if all parties of a contract behave the way it is agreed, to validate their rights, to fulfil their obligations and ensure that no one can misuse information is key for a trustful relationship.

Computable contracts aim to easy the complex processes of contract design, contract negotiation, contract signing, contract termination as well as to observe the fulfilment of contractual obligations and compliance with national law."[296]

[296] https://gaia-x.gitlab.io/technical-committee/architecture-document/conceptual_model/.

Figure 10: Gaia-X contract-as-service template



Source: Gaia-X Data Contract model template

CashOnLedger is not an owner/operator but rather an infrastructure provider of services that incorporate blockchain technology with data-driven insights from telemetric sensors. This data is compatible with the ERP and accounting-based software of the companies that use CashOnLedger technology for asset life-cycle management. Therefore, the contracts entered into between consenting parties are traditional contracts at law drafted by lawyers and do not exist on chain, or in hybrid format as Ricardian contracts.

Regarding Bosch, it is unclear from the interviews to what extent the moveID project makes use of conventional contracts at law. As the primary goal is related to data portability for the IoT sector, the use of blockchain and smart contracts is being investigated to harmonize use in situations where human beings are not the only reference point. To the extent that the smart contracts facilitate data exchange, the rules governing Gaia-X also in relation to Federated Catalogues and data marketplaces remain in scope. Bosch has mentioned that the legal aspects related to moveID are currently being explored also with academic partners, although the specifics of this are not publicly available beyond said partnership announcements. The details of the work package likely contain research that at this early stage is economically beneficial to the moveID consortia.

- **E. Challenges arising from court/dispute resolution.**

Depending on the protocol, smart contracts can be coded using a variety of programming languages. For example, deltaDAO supports the Polygon blockchain which can be programmed using Golang, Solidity or Vyper, while CashOnLedger supports Java Kotin and Solidity. The moveID project is chain agnostic with competing blockchain networks being tested for various use cases. For courts, it is important that smart contracts are auditable in terms of programming logic and performed transactions. It happens that sometimes developers may outsource programming logic to a central server which might disappear. After the delivery of a court decision, it would be beneficial to have an updateable smart contract to implement it (alongside troubleshooting bugs and other necessary changes).

Reading source code is a skill reserved for developers and those with technical knowledge to make sense of the underlying logic. Member States raised the question of how smart contracts could be read accurately and successfully in a court of law. It was argued whether judges in particular can be said to possess the necessary skillsets to make use of smart contracts in legal proceedings when rendering verdicts, opinions, or dissents. Another important question concerns what can and could be done if a court decides that the functioning of the smart contract should be changed, updated or terminated. As described under section D, contracts used in the deltaDAO operating model presuppose that the participants establish a legally binding act before any service offering or transfer of data to the data consumer. This B2B contract has the option to be governed under Union or EU/EEA/Member State law, including the requirement to have contracts also in written form. Moreover, there exists a general protection under EU law normally applicable that cannot be avoided through the choice of law for B2C contracts according to Article 6(1) of the Rome I Regulation, which stipulates that the applicable law for B2C contracts shall be the law of the country where the consumer has his habitual residence, provided that the business/trader: (a) pursues his commercial or professional activities in the country where the consumer has his habitual residence, or (b) by any means, directs such activities to that country or to several countries including that country, and the contract falls within the scope of such activities. Moreover, Article 6(2) sets out safeguards for the further protection of the consumer by stating that even when the parties choose the applicable law, “[S]uch a choice may not, however, have the result of depriving the consumer of the protection afforded to him by provisions that cannot be derogated from by agreement by virtue of the law.”

Section C has noted that Gaia-X Self-Descriptions are defined using human-readable JSON-LD files (a deeper analysis on the use of JSON files in human arbitration and e-discovery is presented in section 3.3.2). It is also impossible for a participant under the Gaia-X Trust Framework to forgo adequate KYC/KYB verification. The verifiable credential used to authenticate users and legal persons must also be human readable in the event of a breach in the terms and conditions. For example, if an individual or legal person lies about their GDPR or ISO certification as part of the verifiable credentials in their self-description, authorities which can issue audit trails can be called on for disputes. Spending of data tokens creates additional audit trails as it instantiates the service offering, which may be used in the event of arbitration.

Court/dispute resolution faces less obstacles in regard to CashOnLedger, with traditional contracts being drafted between counterparties. Here, CashOnLedger and its associated technical model provide infrastructure solutions. There is no immediate challenge to human or court arbitration in the event of disputes. CashOnLedger also maintains control of the node infrastructure and data flows (see section J for detail). This data is cleaned and uploaded through the Quorum notary function in Excel files which are easy to read and understand. In the event of a situation where legal recourse or arbitration is necessary, this data could be used in e-discovery or trial proceedings. With Bosch, challenges arising from outside the scope of autonomous agents could make use of the Gaia-X Self-Descriptions (see also C.1 and E.1) within the Gaia-X Trust framework. There currently exists no reliable precedent for a court arbitration to make use of smart contracts in such cases involving autonomous agents. The robustness of the code would also need to be verified in order for the outcome from a smart contract to be reliable enough for court arbitration.

In order for smart contracts to be 'read' and understood in a judicial review in court/dispute resolution, it is an advantage if they are archivable, including the transactions and logic in a trusted form for the court. In such cases, part of the transactions could be stored with a corresponding part of the logic moved to a separate and dedicated node. The code could be archived as well, while the programming libraries remain unavailable. Other examples of work being done to bring blockchain into court proceedings include the four-stage process designed by Low (2021) following a method of zero to full implementation on-chain:[297]

1. "A judgement issued by a national court[298] specifies payment in cryptoassets. There is no particular interaction with the blockchain and parties must get the judgement recognized in the executing jurisdiction through the traditional recognition process.
2. A judgement issued by a traditional court specifies payment in cryptoassets. Judgment orders are recorded on-chain allowing the judgment to be more easily recognized in the executing jurisdiction using blockchain evidence of the judgement. If the judgement is made off-chain, oracles could receive judgement data off-chain and transmit this to a smart contract.
3. A judgement issued by a traditional court specifies payment in cryptoassets. Parties entered into a dispute resolution smart contract automating judgement execution. Those orders are communicated to the smart contract either through off-chain through an oracle or already recorded on-chain.
4. The court may oversee a judgement issued on chain pursuant to a blockchain dispute resolution process. Original transaction subject to the dispute is also recorded with a dispute resolution protocol in the smart contract triggering court involvement already in place. Parties may also enter into a new dispute resolution smart contract to automate judgement execution."[299]

The spectrum of possibilities also raises other questions which need to be addressed:

- Establish a conflict of laws analysis in case blockchain-executable judgements cannot be issued under a given law.

[297] Zhen Er Low, Commentary, *Execution of Judgements on the Blockchain- A Practical Legal Commentary*, Harv. J.L. & Tech. Dig. (2021), available at: https://jolt.law.harvard.edu/digest/execution-of-judgements-on-the-blockchain-a-practical-legal-commentary.

[298] Questions regarding the robustness of smart contract, archiving, auditability, updatability, governance and termination would still remain open in this case.

[299] Ibid.

- Gain access to a dispute resolution protocol, providing evidence of implementation early in the court process.
- Courts may need to provide template code for commonly used blockchain systems (e.g., payment of transfer of title). This could be done in collaboration with tax authorities, governmental registries and other appropriate use-case specific bodies.
- Complex remedies (e.g., prior confirmations of fact or interim orders) may require a larger repository of templates from an advanced court system.

A larger database could provide some clarity for precompiling code related to post-judgement appeals (stay of execution tied to appeal time limits), that are subject to extension of time orders from the court. Blockchain based dispute resolution could also reduce the likelihood of antisuit injunctions in cases with suits conducted in concurrent jurisdictions. In such cases, the court of first commitment would end up prevailing.

Globally, there are companies already building blockchain dispute resolution including Kleros, Jus, Aragon and Oath protocol.[300] These platforms operate via blockchain jurors that decide cases through staking tokens or building credit.[301] The Hangzhou Court also has a system for e-commerce disputes, online contracts and internet copyright infringements.[302] The end-to-end platform allows pre-identified contracting parties to execute smart contracts recording their original transactions. Once activated, dispute conditions can send a case to mediation then a court hearing by a national court. The judgement ties into the larger framework of China’s social credit system. It should be made clear that the use of blockchain technology in China has been uniquely tuned to suit the system of government enforced by the People’s Republic. Therefore, a distinction should be drawn in normative terms between how DLTs operate in China vs. how they are normatively viewed (and designed) in Western democracies. In the United Arab Emirates, Dubai and Abu Dhabi are also contemplating the ‘Court of the Blockchain which was launched in 2018 as a collaboration between Dubai international Financial Centre (DIFC) and Dubai Future Foundation (DFF) which aims to build on existing dispute resolution services, exploring how blockchain can be incorporated to allow different exceptions and conditions, aiding in cross-border judgements.’[303]

As the examples above highlight, blockchain based dispute resolution is beginning to find ground as a means of Alternative Dispute Resolution for C2C cases, alongside individual national pilots. The rise of blockchain based dispute resolution systems is therefore a cross-border phenomenon with international dimensions. The adoption of such systems should be considered as a trade-off between the benefits of automated execution within a blockchain-based dispute resolution against the opportunity cost of any funds being restricted by time spent in litigation. As noted by Low (2021), the biggest obstacle to adoption remains legal recognition of blockchain based/incorporated judgements at the national level. To the extent that blockchain jurors, dispute resolution and smart contracts aided in court proceedings can guarantee a right to an effective remedy at the European or

[300] Ibid.

[301] Jenny Vatrenko, *The Lay of the Land in Blockchain Dispute Resolution and Governance Designs*, Hackernoon Blockchain Governance (Jan. 16, 2019), available at: https://hackernoon.com/the-lay-of-the-land-in-blockchain-dispute-resolution-and-governance-designs-6e858004e444.

[302] Miranda Wood, *Chinese internet court adopts blockchain smart contracts, processes 1.9bn transactions*, Ledger Insights (Nov.2017), available at: https://www.ledgerinsights.com/chinese-internet-court-blockchain-smart-contracts/.

[303] David Savage, *Thoughts for the new decade: smart contracts, blockchain and construction dispute resolution*, Thomson Reuters Prac. L.Construction Blog (Jan.14, 2020), available at: http://constructionblog.practicallaw.com/thoughts-for-the-new-decade-smart-contracts-blockchain-and-construction-dispute-resolution/.

national level depends on whether they are in practice compatible with specific legal protections. For example, the first paragraph of Article 47 of the EU Charter of Fundamental Rights is based on Article 13 of the European Convention on Human Rights (ECHR) and being read in connection with Article 6 ECHR – ensures that "Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article."[304]

The European Court of Justice in *Johnston* 1986 enshrined the right to an effective remedy with a focus on seeking judiciary relief before an actual court as a general principle of Union Law (see also *Heylens 1987, Borelli 1992*). In the case of blockchain jurors where the dispute resolution is not tied to a verdict rendered[305] it does not preclude the parties from seeking further remedy under court of first instance. [306] Given that these dispute resolution platforms using blockchain jurors are typically operated by private companies, the parties may question the impartiality and/or independence of the tribunal as it is not 'established by law' in the context of arbitration bound also by the rules of the New York Convention on Arbitration. Furthermore, if the blockchain based dispute resolution was initially undertaken within a national court it follows that the parties can challenge this in an appellate procedure. In *'Les Verts' v European Parliament*, the European Court of Justice held that the right to a fair hearing is not relegated solely to disputes involving civil law rights and obligations. Therefore, any application of similar technological and legal pathways in the EU would be bound by the same horizon of possibilities.

Further, it was established in *Airey v. Ireland*, and in accordance with the case-law of the European Court of Human Rights that legal aid should be made available where the absence of such aid would mitigate the ability to ensure an effective remedy. To the extent that a blockchain juror system operated by a private company mandates the deposit of tokens into an escrow smart contract before jurors can render a verdict, and this platform does not ensure for example a 'legal aid fund' within its terms and conditions, it could be found in violation of Article 47 of the EU Charter of Fundamental Rights. Conversely, such legal aid would need to be available to parties if blockchain based dispute resolution were applied in national courts.

F. Clarity and Interpretation of legal terms (including the addition of specific and/or individual provisions).

Legal desk research has identified that interpreting nuance within legal terms such as 'good faith' or 'fair value' and how it relates to the intent of the parties may be difficult to determine using pure code. It stands to reason that 'if x then y' statements make it complicated to explain nuance. Written contracts can also much more easily define specific or individual provisions (such as subjective or positive qualities related to a good or service), which could also prove difficult to code into smart contracts.

As described in the preceding sections, deltaDAO makes use of both written form and smart contracts to bridge a legally binding act off-chain from how the data on-chain is treated between different participants in the Gaia-X ecosystem. The Gaia-X Policy under 'General material requirements and transparency' also notes that "*the provider shall ensure*

[304] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT
[305] Selective in the sense that the parties opt for a procedure outside the national court system.
[306] A court of first instance is a trail court of original or primary jurisdiction where a case is tried, instead of being heard on appeal.

there are specific provisions regarding service interruptions and business continuity (e.g., by means of a service level agreement), provider's bankruptcy or any other reason by which the provider may cease to exist in law […] the provider shall ensure there are provisions governing changes, regardless of their kind."[307]

Service Offerings make use of the Open Digital Rights Language (ODRL) which is a policy expression language that provides a flexible and interoperable information model, vocabulary, and encoding mechanisms for representing statements about the usage of content and services. It falls under W3C Recommendations. ODRL is split between Policy Class, Asset Class, Party Class, Action Class, and further define constraints and rules.[308] As an example, policy subclasses can be mapped to JSON-LD type tokens, and the logic is also human readable via the JSON format.

Table 7: Service Offering Template

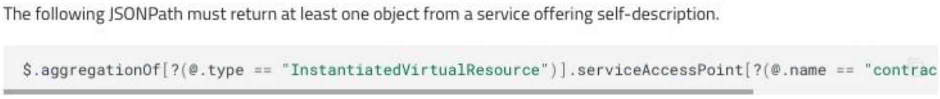
Attribute	Cardinality	Trust Anchor	Other
name	0..1	State	Human readable name of component
providedBy	1	State	Resolvable link to the participant self-description providing the service
aggregationOf[]	0..*	State	Resolvable link to the resources self-description related to the service and can exist independently of it.
dependsOn[]	0..*	State	Resolvable link to the service offering self-description related to the service and can exist independently of it.
termsAndConditions[ ]	1..*	State	Resolvable link to the Terms and Conditions

[307] https://gaia-x.eu/wp-content/uploads/2022/05/Gaia-X_Policy-Rules_Document_v22.04_Final.pdf.
[308] WRC Recommendation, ODRL Information Model, February 15, 2018, https://www.w3.org/TR/odrl-model/.

			applying to a given service.
policy[]	1.. *	State	List of policy expressed using a Domain Specific Language (DSL) (e.g. Rego, ODRL).
dataProtectionRegime[]	0..*	State	A choice of data protection regime
dataAccountExport[]	1..*	State	A list of methods to export data from user account out of the service.

The Service Offering also needs to point to a valid InstantiatedVirtualResource self-description with at least one serviceAccessPoint with a name ‘contractNegotiationEndpoint.’ The corresponding output from the ‘contractNegotiationEndpoint’ must point to the result of a negotiation which was signed by all participants who were in direct link to the negotiation.

Figure 11: JSONPath for validating contractNegotiationEndpoint



The following JSONPath must return at least one object from a service offering self-description.

```
$.aggregationOf[?(@.type == "InstantiatedVirtualResource")].serviceAccessPoint[?(@.name == "contrac
```

Source: Gaia-X services and subclasses

Sections D and E outlined that CashOnLedger sits outside the contractual framework of its current largest operating use-case involving Lindner and participating banks. CashOnLedger facilitates the back-office reconciliations and allows for optimizing existing real assets to be turned into financial assets through tokenization. The contracts between Lindner and participating banks are traditional contracts at law. There is no immediate risk of confusion with interpreting legal terms including the addition of specific and/or individual provisions. Smart contracts are also used in different specificities. CashOnLedger has a narrow payments/reconciliation focus while smart contracts deployed under moveID depend on the specific type of blockchain network and associated use case optimized for mobility solutions. These could range from data portability from sensors to autonomous agents, portability and ownership of data from Self-Sovereign Machine Identities (SSMIs) to transactions conducted independently by these SSMIs. It is difficult to identify exactly at this stage what contract provisions including clarity of terms are directly in scope for smart contracts.

The moveID cluster uses smart contracts to optimize automation gains and create use-cases for yet to mature industrial applications that currently suffer from a general lack of legal foundation internationally, including Europe. As discussed in section E, the case studies are only able to bridge the technical/legal gap to an extent. Some, like

CashOnLedger choose to rely on established rules and contractual terms. This is also because CashOnLedger operates in an ecosystem also dealing with financial services and is positioned as a go-between for those operators and financing parties that also touch on this sector. MoveID faces other more forward-looking challenges due to the nature of the ecosystem it is building service infrastructure for.

There are other market-based solutions outside the case studies being explored for overcoming barriers between code and semantic text. Hazard and Haapio (2017) proposed an extension of smart contract templates through 'prose objects' and prototype inheritance demonstrated at CommonAccord.[309] There are also markup languages like LegalXML and LegalRuleML which yield data schemes/rule interchange language for the legal world. However, markup languages do come with drawbacks:

- The semantics of an agreement are only known to the extent that they can be expressed in the tags attached to the legal text, and for the particular meaning for which the tag already exists.
- Contract clauses may be too complex to express in simple tags. A solution could be to provide simple semantic tags to simple text elements. This would allow one to define the general analysis, determining the semantics for each clause from its elemental semantics.
- There is always a risk that the code is written in a programming language too complex for either party to read.
- The code is still logically separate from the contract.

For smart legal contracts what is still missing from the market is a Domain Specific Language (DSL) that could combine in one artifact the smart contract and contractual obligations. Another line of thinking is more of an edge case. In theory, the contract could be the source code. Source code can contain textual data objects of varying complexity allowing the code to define a text object which could define the entire natural language contract. Specification languages can express deontic aspects (e.g., rights, obligations and permissions) which the legally binding smart contract could monitor. Specification languages also allow temporal constraints and other operational questions to be expressed alongside recording definitions.

G. Immutability, reverse transaction features and safe termination

Smart contract immutability was a common concern identified in the legal desk research. Cases where an invalid clause can continue to self-execute, causing a problem of unjust enrichment under Article 9(1) CRD were cited. Not all blockchains operate with the same smart contract logic, and blockchains can be public permissionless, public permissioned, or private permissioned. Smart contracts aim to ensure the proper fulfilment of obligations and due to their technical format, can mitigate the risk of dishonesty by the parties. For example, failure to fulfill an obligation may happen due to technical error – especially in smart contracts that are not upgradeable. Obligations fulfilled in error require the application of bilateral restitution, which may be possible through a reverse transaction mechanism provided for in the smart contract. Although not directly related to the draft Data Act, due to their potential impact on smart contracts, part of this section outlines the

[309] James Hazard and Helena Haapio, Wise Contracts: smart contracts that work for people and machines. *Erich Schweighofer et al. (Eds.), Trends and Communities of Legal Informatics. Proceedings of the 20th International Legal Informatics Symposium IRIS 2017. Österreichische Computer Gesellschaft, Wien 2017, pp. 425–432, February 2017.* *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2925871*

possibility of reverse transactions within the case-studies. Section A.1 techno-economic Implications takes further stock of reverse transactions in the broader context of the blockchain ecosystem. As regards safe and robust termination, Article 30 of the draft Data Act requires that the vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of an agreement to make data available has to ensure that smart contracts are robust, that they ensure safe termination and interruption, data archiving and continuity as well as access control.[310]

Reverse transactions are the ability to cancel or reverse a pending transaction on a smart contract. In an IT context, ensuring safe and robust termination can be understood as a mechanism used to shut down a device or program. For the purpose of this study such methods refer to the ability to intervene in a smart contract and halt/reverse a given programmable function for the purpose of changing the outcome of the smart contract; in effect circumscribing its immutability. The degree of openness of a blockchain network may determine whether there is a technical penalty that risks the fidelity of the network if a reverse transaction were to be carried out. Different use cases may simply not require them at scale and regulatory and legal constraints also create an added layer of complexity.

deltaDAO does not directly make use of reverse transaction features or safe termination. However, the underlying blockchain Ocean Protocol through which the data token model is orchestrated has a function called 'data asset purgatory' which behaves like a kill switch. It allows Ocean data markets to handle IP violations and sensitive data. The Gaia-X framework makes use of more targeted onboarding requirements (Verifiable Credentials under Gaia-X are vetted through Trust Anchors with public level API reference data while Ocean Protocol Verifiable Credentials are only linked to Ethereum Name Service addresses). This mitigates the need for reverse transaction features and safe terminations. The smart contract logic instantiates the Verifiable Credentials and porting of the data token, but the governance terms are first set in the conventional law, which is then transferred to code. The use of the data token is first drafted under a standard written-form contract.

Quorum, the blockchain that CashOnLedger has used to build its service offering has transactions that include three parts:

- Global transaction hash
- Public state root hash
- Block maker's signature

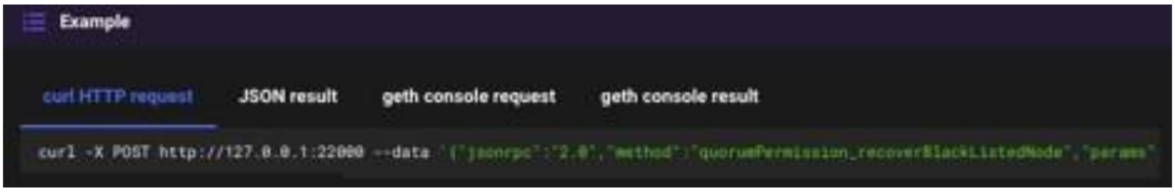
The Quorum network also contains a voting consensus mechanism which delegates voting rights to voting nodes. Quorum tracks the status of all voting nodes and works as a majority voting protocol. Transactions are completed if they receive a majority of the votes. Therefore, in theory a transaction can be reversed or denied if it fails to receive a majority of votes from the network nodes. Nodes can also be blacklisted from a set of Quorum-able nodes provided by developers. It lets user wallets deny engaging with nodes that a user specifically does not trust.

However, these blacklisted nodes can also be 'called back.' The quorumPermission_recoverBlackListedNode function will initiate the recovery of a specific blacklisted node. This methodology can be called using a network administrator account.

[310] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068

Most network administrator accounts are needed to approve a blacklisted node as active again.

Figure 12: Node recovery on Quorum



```
curl -X POST http://127.0.0.1:22000 --data '{"jsonrpc":"2.0","method":"quorumPermission_recoverBlackListedNode","params"
```

Source: Consensys

State verification is important to mention here. In Quorum, validating a block includes a check on the root of the public state to determine if it is synchronized across nodes. This will also include a check on the global transaction hash, letting each node validate that they have the same set of transactions as the other nodes. Synchronizing the public state root and private transaction inputs may imply a synchronization of the private state across participating nodes. However, this model restricts the ability to change public state in private transactions. Private transactions are commonly used to read data from public contracts so the virtual machine will change to read-only mode for each call from a given private contract to a public contract. If the code tries to make a state change while the virtual machine is in read-only mode, the virtual machine will stop executing and flag an exception. CashOnLedger further articulated that once a use case is deployed, it has a large off-chain legal foundation behind it which constrains the activities of users operating inside the permissioned network. This acts as a primary deterrent for any untoward behaviour on chain.

It is yet unclear whether reverse transaction features are possible in the moveID project. Research is underway using several different blockchain networks. Each of these has a different implementation in practice. It stands to reason that depending on the deployment of the smart contract and type of blockchain network; a reverse transaction may require different network needs and carry a different associated cost.

As this report has mentioned, Self-Sovereign Machine Identities (SSMIs) do not currently have a legal standing at European (or member state) law. In the event SSMIs could possess eIDAS compliant wallets, a remote wallet safe termination could be integrated for wallets operated by autonomous agents. If a vehicle or smart censor became corrupted, there could exist a need to lock its ability to transmit incorrect data (a traffic sensor malfunction) or cancel a pending payment (malware downloaded into a car). This would also serve to protect the eIDAS credentials held in the wallet. Another option is to revoke specific credentials within the wallet rather than terminate it full stop.

Bosch has associated technology that can be used within moveID for hardware security to be viable in place of reverse transactions. At the hardware level, Bosch electronic control units have a hardware security module where cryptographic keys can be securely stored. Bosch has a global key management system which places the keys during manufacturing. moveID also makes use of software-over-the-air (SOTA) updates. These types of updates can be done in stages years after a vehicle has left the factory to keep pace with cyberthreats as they become more sophisticated, further calling into question the need for the upgradeability of smart contracts.

From a legal standpoint, the immutability of a blockchain is at odds with certain obligations including not least of which consumer safety. Immutability is also the underlying instrument that makes blockchains commercially viable in the first place. As the Draft Data Act seeks to ensure the safe and robust termination of smart contracts, it is unclear how compliance will evolve at the developer level. Although concepts like Ocean Protocol's data asset purgatory, or smart contract 'self-destructs' exist; the key takeaway is that not all distributed ledgers are the same. In practice, implementing safe termination may be more viable in private-permissioned chains where the parties in the network are already subject to strict oversight. At present, many such on-chain environments take place between regulated financial intermediaries where financial services regulation is dominant and the DLT application is B2B. For example, CashOnLedger built their service offering on Quorum because of its network security and unified data source. The network contains regulated banking institutions which use CashOnLedger to optimize back-office redundancies. Transactions in Quorum can be segregated which increases their overall security.

Smart contracts may also be 'modified' although not strictly in the sense of ensuring safe termination. One such example would be a 'pointer' contract referencing the old one. Smart contracts deployed using Open Zeppelin Upgrade Plugins can have their code modified while at the same time preserving their state, balance and address. Smart contracts can also be upgraded on Solidity using different methods:

- Proxy contract using delegate call.
- Using an interface pattern to call a function in another contract.
- Storing all data in a storage contract: using one contract to store all data and another to store all business logic. Functionality cannot be manipulated in the storage contract, but the business logic contract is replaceable.

Node allocation is another point to consider. Nodes relate to influence on the network which is proportional to counterparty risk (in the case of master nodes). The ability to implement reverse transactions and/or terminability can still succumb to human error or ignorance, unintentionally triggering financial losses. It is also evident that the shift towards Industry 4.0 means smart contracts are not operating in a vacuum. The growth of the Internet of Things (IoT) sector brings additional complexity. Smart contracts are not only facilitating transactions between natural persons, but increasingly being designed for use between machines. Sensors, autonomous vehicles and smart devices are being calibrated to receive/transmit data to each other, identify each other and pay for services. Applying terminability to blockchains needs to be considered in the context of how this could impact European competitiveness within Industry 4.0, where the scale and complexity of various machines and sensors, each with their own version of software not only might require changes for smart contracts, but could lead to additional cybersecurity risks – requiring yet more updates to keep pace.

H. Evidential Value of Documents

Member States had different thresholds on what constitutes full evidential value. The most common were in relation to the use of qualified electronic signatures. These measures ensure the drafted document is stored in a way that guarantees its integrity. Smart contracts may qualify as electronic contracts as defined under the eIDAS Regulation. As such, they require an advanced electronic signature also conforming to the requirements laid down under eIDAS to have full evidential value.

Section C outlined the process through which Verifiable Credentials issued under the Gaia-X Trust Framework get validated. For an attestation to be successful it must be verified by a Trust Anchor. These Trust Anchors must be eIDAS certified bodies such as a state validated entity issuer or an EV SSL if the participant with a legal address is in the EU/EEA.

All key pairs that are used to sign claims need to incorporate at least one of the listed Trust Anchors in their certificate chain to remain compliant with the Gaia-X Trust Framework. The Gaia-X Policy Rules and Labelling Document also indicate that in the event of non-compliance with the Trust Framework, key pairs that are used to sign Verifiable Credentials will be revoked by the Gaia-X Association.

There are no obstacles to the full evidential value of documents also in the case of qualified e-signatures in the CashOnLedger case study as the contracts are conventional contracts at law. Insofar as full evidential value of documents also related to qualified e-signatures, this is an area where Bosch also sees a need for further clarity at European Law for the attestation of SSMIs and their provision of eIDAS compliant wallets. Otherwise, the Gaia-X Trust framework (section H) applies in cases other than autonomous agents (see also Techno Economic Implications B.1. European Blockchain Services Infrastructure use cases).

Where the use of smart contracts qualifies as an electronic document bearing full evidential value (e.g. IT, GR), qualified e-signatures such as those under the Gaia-Trust Framework would face less obstacles. In Austria, using public authorities as Trust Anchors may be a way to overcome the 'in-between' barrier as Trust Anchors issue qualified attestations for KYC/KYB under Gaia-X. CashOnLedger relies on distributed ledgers for only 10% of its product offering and bases its contractual business relationships using standard written-form contracts. The biggest obstacles to full evidential value, including in the use of qualified electronic signatures, are found in moveID. Given the consortia focuses on applying different blockchain networks to solve identification, verification and use of machines in mobility solutions, challenges are beyond the lack of recognition of smart contracts. Such challenges are also in terms of the validity of machine identities and whether such identities may be considered in future iterations of the eIDAS framework.

I. Embedded supervision

Having a high-level view and the ability to embed regulation at the infrastructure or market level is viewed as a potential gamechanger for ringfencing any drawbacks associated with using smart contracts. In this regard, embedded supervision has been highlighted as an area worth exploring. Embedded supervision entails a conceptual regulatory framework that allows for compliance via automatic monitoring of decentralized markets. This is achieved by reading the state of the ledger that supports a given market which uses smart contracts. It is designed in such a way that limiting the scale inherent in decentralized exchange could be overcome by having applications running on 'permissioned' DLT. Peer-to-peer exchange would be driven by decentralized economic consensus. The use of on-chain data could then replace intermediary-based legal data verification. In some cases, it may also presuppose exchange between regulated entities and is considered in the context of an entity-based regulatory framework (i.e., the relationship between the underlying asset and the digital token must be guaranteed by the legal system).[311]

The Gaia-X Label Framework distinguishes between Label Owners and Label Issuers. Because the baseline for a Gaia-X label is defined by the potential use and benefit of it, actors can define specific labels to suit their needs. They can also ensure that the cloud adopted by their associates will conform to specific requirements and which requirements

[311] Raphael Auer, Embedded Supervision: how to build regulation into decentralized finance. BIS Working Papers no 811, 2019, https://www.bis.org/publ/work811.pdf.

may need to be verified (jurisdiction, certifications, the location of the service). For actors in a private consortium using the infrastructure or service offering, there could exist a need for a form of supervision although from the case study interviews it is unclear what form this would take. On-chain transparency is currently live by default, and everything is public. This makes it easy to follow audit trails and target individual instances of non-compliance. Further, a service provider is directly responsible, and by default liable for the smart contract instantiated for a given service. Moreover, that smart contract is created specifically for that purpose and that service offering. Once the consumer spends it according to the terms and conditions it creates an audit trail. Thus a de facto form of 'embedded supervision' already exists by nature of the network's transparency.

With CashOnLedger one could understand 'embedded supervision' at the hardware and network levels respectively. To create a false truth on chain, all tractors in Lindner's case must be tampered with to alter the single source of truth. Thus, a single source of truth that is authentic starts at the chip level. Just as penetrating the network would start with the chips, supervision working in reverse would do so as well. In theory, all telemetric units would need to be simultaneously calibrated while the payment data on chain would also need to be calibrated in parallel. This combined data could then be delivered to banking supervisory authorities, insurance companies and others in the network's value chain based on the priority of that data for its intended purpose. An example would be banking supervisory data going to supervisory authorities while perhaps insurance sensitive data going to insurance companies. This would require those bodies to operate nodes within the network. However, operating network nodes is a sophisticated process. It requires technical knowledge, time and resources to maintain at scale.

This is a task and associated risk that the banks and insurance companies CashOnLedger has been working with are not willing to take on a present. For that matter, Lindner does not operate its own nodes either. At present, CashOnLedger acts as the service provider and de facto network administrator. The data sets are first cleaned and imputed, then downloaded into excel files before being manually ported to the parties involved. This is done because they lack the tools and internal controls needed to utilize and make sense of the raw data files. Further, because this excel data is then accessible through the notary function available in Quorum, the banks in particular are not motivated to take on any new risk. Embedded supervision was mentioned by Bosch as a potential way to ensure compliance with existing laws and regulations while protecting consumers. The means to achieving it, however, are not yet clear within the mobility domain. A concept roadmap for different entry points for embedded supervision is outlined below. Important to note is that the built-in transparency of the network allows for most of what constitutes 'embedded supervision' to be undertaken through on-chain analytics and leveraging the visible data across the network.

Table 8: Hypothetical embedded supervision for mobility

Process	Supervisory entry point
Agents can directly discover each other without relying on centralized solutions.	On-chain verification for agents in the network.
Agents use smart contracts to execute standardized transactions.	On-chain monitoring of transaction data.
Smart contracts can be used for payments + point to off-chain solutions for data storage.	On-chain monitoring of transaction data, also potentially feeding back to API frameworks set up for supervisors.

E-wallets/agents in the vehicle allow for offline discovery and contracting.	Potential monitoring of un-hosted wallets set up for autonomous transactions.
Nodes across an ecosystem communicate on decentralized marketplaces and may carry agents and/or e-wallets.	Role for supervisors to access relevant node data and/or serve as a validating node for regulatory purposes.

What is clear about embedded supervision is that in theory it is possible across all three case studies and within the wider market. The definition of 'embedded' in embedded supervision may have to change with regards to the specific blockchain network and use case. This has to do with the fact that public/private chains are built with different node functionalities and operational requirements. DLT networks employed in financial services use cases are already subject to much stricter oversight. With the introduction of EU public level oracle frameworks, it may be a way to transmit hard, cheap and static data to the blockchain which is compliant. The takeaway from the case studies is that embedded supervision does not simply stop at on-chain tracking but could also move into the hardware level. In the case of CashOnledger this could result in additional costs and counterparty risk to network participants. Embedded supervision need not be prohibitive but can use the built-in transparency and real-time data insights of distributed ledgers to monitor compliance.

3.3.2. Techno Economic Implications

This sub-section assesses the current control methods for smart contracts and the way regulatory tools impact the underlying blockchain, developers and users. The robust matrix compiled while carrying out the technical feasibility assessment (see Annex III) will further inform the range of techno-economic implications. Technical feasibility solutions in the previous sub-section can be grouped across two main streams: A) Infrastructure, security and consumer protection and, B) Data portability and decentralised identity as shown in the table below.

Table 9: Technical feasibility solutions

Infrastructure, security and consumer protection	Data portability and decentralised identity
Reverse Transactions	W3C Verifiable Credentials
Safe Termination	SoulBound Tokens
Embedded Supervision	Zero-Knowledge Proofs

Using a comparative approach, a feasibility analysis will be undertaken for wide scale implementation and enforcement of identified tools by incorporating the bulleted points:

- An analysis of the pros and cons to identified technical approaches.
- Estimation of efficiency and effectiveness of technical measures.
- Estimation of security of analysed technical measures (critically tied to stakeholder protection).
- Techno-economic and strategic implications of specified approaches to code – based consumer protection regimes.

Finally, a conclusion will be drawn from the provided analysis for each aspect of the subtask.

A. Infrastructure, security and consumer protection

The use of reverse transaction features and safe termination are advanced as a way to make smart contracts safer from a consumer protection standpoint. In parallel, the draft Data Act under Article 30 makes smart contract terminability conceptually obligatory on the grounds that self-activating or autonomous code (in some cases) can be harmful to users. The Data Act does not directly cover reverse transactions. However, due to their far-reaching implications, both solutions are discussed in the broader context of the blockchain ecosystem as they would apply to cases concerning notably public permissionless proof-of-stake consensus.

1. Reverse Transactions

According to the cryptoasset intelligence company Chainalysis, cross-chain bridge hacks became the number one smart contract security vulnerability in 2022.[312] Cross-chain bridges are implemented to overcome interoperability challenges that exist between different blockchains and let users transfer cryptoassets from one blockchain to another. For instance, these could be transfers of cryptoassets or NFTs between Ethereum and Solana, as in the case of the Wormhole cross-chain bridging protocol. In principle, bridges work by receiving funds in one asset to the bridge protocol which get locked into a smart contract. A user would be issued funds in the equivalent for a parallel asset on the chain the protocol is bridging to. Bridges can feature a central pool of funds backing bridged assets on the receiving blockchain. This makes them vulnerable regardless of whether they are locked in a smart contract or held with a custodian.

In other cases, a protocol's native token can be manipulated, as was the case with the Mango Markets hack using the native MNGO Token. Mango Markets is a decentralised finance (DeFi) trading platform operating on the Solana blockchain which saw an exploit of US $116 million in liquidity from all available tokens. The hack was achieved by using two different accounts, one taking a short and another a hedging position. The attacker initially deposited around 5 million USD Coin (the payment stablecoin issued by Circle) to the network and then opened a long position. Next, the attacker bought 438 million MNGO Tokens (the native token on Mango Markets). This made the price of the MNGO Token rise by 1000% and elevated the collateral value of the hacker's account.

Once stolen, tokens can be siphoned off between multiple accounts, sold off to unsuspecting buyers or distributed through mixers which obfuscate the destination of ERC-20 tokens. Taken together, such cases provide an argument for features such as reverse transactions or rollbacks.

In a 2018 Twitter comment, Ethereum founder Vitalik Buterin opined that "someone should come along and issue an ERC-20 reversible Ether that is backed 1:1 by Ether but has a DAO[313] that can revert transfers within *N* days." Recently, researchers from Stanford University proposed such a concept in a working paper.[314] The smart contracts are notated ERC-20R and ERC-721R (for reversible). Wang et. al (2022) designed a high-level

[312] https://blog.chainalysis.com/reports/cross-chain-bridge-hacks-2022/.

[313] Distributed Autonomous Organisation.

[314] Kaili Wang, Qinchen Wang and Dan Boneh, ERC-20R and ERC-721R: Reversible Transactions on Ethereum. Stanford University, October 2022. https://arxiv.org/pdf/2208.00543.pdf

workflow for how to reverse a posted transaction consisting of a request freeze, asset freeze and a trial through a decentralized set of judges.

- **Freeze Request**: A freeze request can be posted to a governance contract including evidence and some stake. Only addresses affected by a transaction can request a transaction freeze.
- **Asset Freeze**: The request freeze can be accepted or rejected by a decentralized set of judges. If accepted, an on-chain governance contract is instructed by the judges to call a freeze function on the impacted reversible smart contract. These assets become frozen and cannot be transferred.
- **Trail**: Evidence is then presented to a decentralized set of judges from both parties to the initial transaction. Once a decision has been reached, the judges instruct the governance contract to call either the reverse or rejectReverse functions on the impacted smart contract(s). A reverse function would transfer any frozen assets back to the original owner while assets are released and unfrozen by the rejectReverse function and left where they are.

Wang et. al (2022) created a Solidity implementation split between the main ERC20R/ERC720R contracts which keep track of all balances and transactions and another governance contract to select judges and gather votes. These implementations are extensions of OpenZeppelin non-reversible contracts.[315]

The same way existing ERC-20 smart contracts manage the balances of many accounts, the ERC-20R contract has an account balance with a pair of numbers notated as Rbalance and NRbalance.

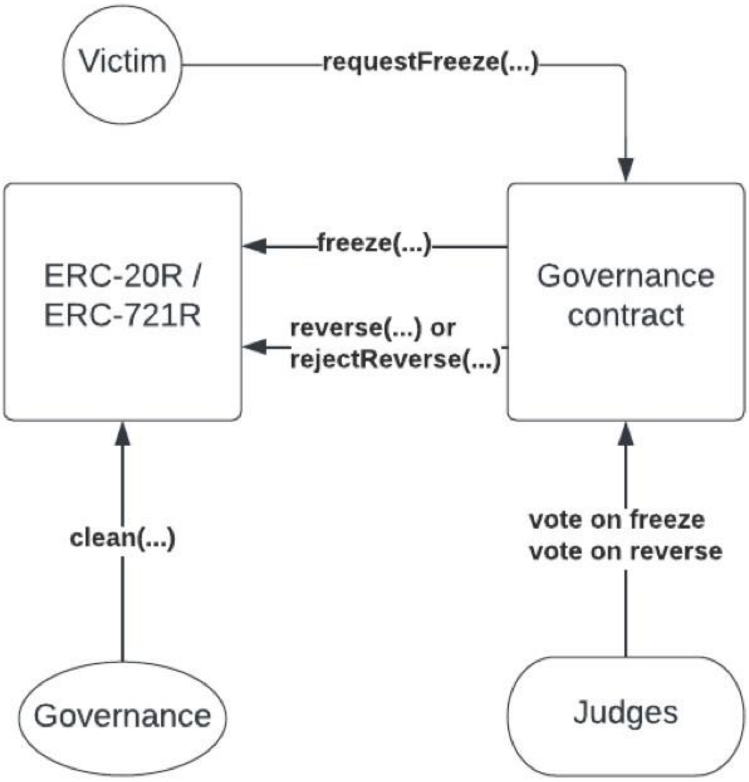
- **Rbalance:** account balance due to recent incoming transactions with funds subject to reversal.
- **NRbalance:** Current account balance with incoming transactions consisting of an elapsed dispute window. These funds are non-reversible.

A ‘clean’ function shifts funds between the Rbalance and NRbalance contracts as the dispute window elapses. Account owners sending funds from their own account to another account can specify how much to deduct from each balance. Wang et. Al (2022) devise an ERC-20 transfer function split between transfer() and Rtransfer().

- **Transfer()**: from non-reversible balance.
- **Rtansfer()**: from reversible balance.
- The transferred funds get added to the recipient’s Rbalance.

[315] OpenZeppelin Contracts is a library for secure smart contract development.

Figure 13: Model for reversing a posted transaction on Ethereum



Source: Wang et. Al (2022)

The transfer function is also backwards-compatible with the current ERC-20 contract standard. ERC-20R is also backwards compatible with current decentralised finance infrastructure like decentralised exchanges (DEXs) and/or lending protocols. Because the ERC-20R's transfer() function has an identical Application Programming Interface (API) as the ERC-20 transfer() function, no software changes are required to process customer requests.

Such a model provides a complicated albeit workable solution for implementing reverse transactions on the Ethereum public blockchain. However, there are drawbacks to consider. Introducing a solution to solve a particular issue in one part of the network invariably introduces a new set of problems downstream elsewhere on the network.

There is already evidence from existing payment solutions that reverse transactions can be costly and promote market abuse. Chargebacks in platforms like PayPal are exploited through so called 'chargeback scams.' PayPal's dispute system lets the attacker overcharge a seller for an item and then request a refund of the excess. Once reversed, the attacker proceeds to use the dispute system to ask PayPal to reverse the original transaction, forcing the seller to lose the overpaid amount. In the model proposed by Wang et. Al (2022), the decentralised judges could easily be flooded with fake reversal requests of a similar nature which would drive up the adjudicating costs when filtering through genuine and fraudulent requests.

In 2021, the estimated cost of chargeback fraud to sellers across traditional payment channels was USD 20 billion.[316] According to the Equifax subsidiary Midigator which is used by merchants to manage chargebacks, the number of disputes in 2021 ranged from 23 - 77,331.[317] If one assumes a high turnover of chargebacks could also apply to ERC-20 and ERC-721 token transfers then Etherscan, the Ethereum Gas (fee) tracker can provide further insight. Gas Fees currently range anywhere from USD 1.97/transaction on the NFT marketplace OpenSea for sales to US $ 5.07/transaction on Uniswap V3 for swaps and as high as USD 34.4/transaction on Compound for collections.[318] Assuming the same volume of chargeback requests as 2021 would yield OVER USD 2.6 million in chargeback fees from Compound alone. Etherscan lists data for almost 50 different protocols. The exact cost of chargeback fraud is difficult to quantify but the hypothetical fees mirror the value that would-be scammers could extract from protocols if this were to be commonplace across the Ethereum ecosystem.

Aside from reverse-transaction fraud, another drawback concerns fungibility. The Ethereum network could face bifurcation. More experienced users would likely opt for non-reversible tokens while less experienced users may enjoy the peace of mind of a reverse opt-in. Provided ERC-20/ERC-721 and ERC-20R/ERC-721R tokens traded on a 1:1 basis, fungibility concerns may be outpaced by wider adoption driven through more optionality.

In practice, it may be difficult guaranteeing such tokens trade at par. One can foresee an example where tokens are transferred between users A and B. User A may prefer non reversible tokens because reversible tokens carry a call-back risk. In order to be compensated in reversible tokens, user A may request additional reversible tokens for the same transaction to satisfy the perceived extra risk. The dispute window would gradually bring the value of both tokens back to par however in the interim they would trade at different prices creating arbitrage opportunities. For example, a dual Ethereum standard may create a new cadre of intermediaries such as brokers or risk appraisers who profit from the purchase of non-reversible tokens by holding them to maturity.

In private permissioned chains, implementing reverse transactions is more feasible. What is required is an agreement among all master nodes to 'roll-back' the ledger. Nodes in a blockchain network are not all the same. For example, master nodes in Proof-of-Stake protocols require a large financial buy-in because they have other features to do with governance and voting rights. Other nodes, such as light nodes validate, store and broadcast data. Therefore, if most of the master nodes with voting rights agree to roll-back the ledger or reverse a transaction it is possible in very specific cases.

Private permissioned chains often operate in environments where a consortium which is already subject to certain regulatory oversight needs added permissions for the purposes of compliance. A network of commercial banks which engage in the cross-trading of derivatives is one such example. Depending on the operational requirements or context of a specific trade on chain, the nodes could be rolled back an hour, day, week etc., based on need. The problematic data could be deleted allowing the chain to carry on unobstructed. In public blockchains this event could be tantamount to a hard fork that would

[316] https://www.juniperresearch.com/whitepapers/fighting-online-payment-fraud-in-2022-beyond.

[317] https://midigator.com/chargeback-report-statistics/#where-did-this-data-come-from.

[318] Gas fees are not static but depend on network dynamics such as the amount of network traffic, supply of validators and demand for transaction verification. Demand, traffic and fees are correlated. https://etherscan.io/gastracker.

split the network and carry economic and governance penalties which could undermine the viability of the entire chain.

2. Safe termination

Terminability and so called 'airgaps' are seen as a way to quarantine the technology and ensure that legal consequences only flow from the legal architecture agreed by the parties.[319] This may include the location of the transaction record and which record has legal effect. The latter destination may not be the smart contract, thereby ring-fencing the legal consequences from technical error. Article 30 of the Data Act states that "the conditions under which a smart contract could be reset or instructed to stop or interrupted, should be clearly and transparently defined. Especially it should be assessed under which conditions non-consensual termination or interruption should be permissible.[320]"

There are cases where terminating smart contracts has been useful. In 2018, Bancor protocol suffered an exploit worth USD 23.5 million.[321] The protocol used its kill switch to reverse ~ USD 10 million of its native Bancor Network Token (BNT) tokens from the hacker. In fact, many early stage blockchain projects implement kill-switches to give developers the ability to react quickly to network breaches. Kill switches also raise questions about risks to decentralisation because they centralise enormous power (and liability) in the hands of developers. The Bancor hack was the result of giving permissions to a wallet address instead of a smart contract. Augur, a decentralised prediction market had a kill switch mechanism, but it was in a smart contract and not a wallet address. The Augur developers chose to transfer all ownership of the kill switch privileges to a burn address – a digital wallet that cannot be accessed because it lacks a corresponding private key.[322] This was done to remove the chances of any centralisation (and liability) over the kill switch from the developers.

Moreover, many important functions of smart contracts are defined and executed according to the 'onlyOwner' modifier. This can be overcome using either a multi-signature smart contract or a model that allows for vote-driven smart contract-based ownership. With multi-signature smart contracts, a minimum number of signatures is required to authorise a transaction. However, much like the case with a wallet address, it centralises authority in those with the authorisations. Hacks can further disrupt the flow of signatures. Community driven voting and governance of decentralised applications may be a way around those shortcomings. In the case where a kill switch is necessary, such as the hacking of a decentralized autonomous organisation (DAO), implementing one could require simple majority and low threshold. DAOs may also need some form of secondary member vote involving the larger community to revoke the state of emergency.

The takeaway from Bancor and this hypothetical example is that the success of a kill switch is predicated on speed. Even still, the risk of human error or ignorance can result in unintentional security breaches that carry financial penalties. Parity, the core blockchain infrastructure company faced a situation in 2017 where its multi-signature wallet suffered a hack. The exploit took place because Parity's library contract was not initialised, leading to

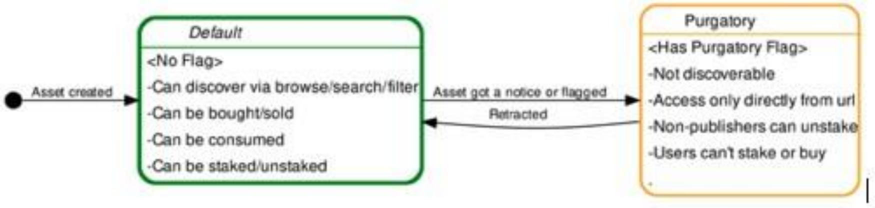
[319] Jason Allen and Peter Hun, *Smart Legal Contracts: Computable Law in Theory and Practice*. Oxford University Press, 2022.
[320] Ibid., Data Act, Art.30
[321] https://www.coindesk.com/markets/2018/07/15/135-million-hack-ignites-fresh-debate-over-crypto-project-bancor/.
[322] https://messari.io/report/augur-burns-the-network-s-kill-switch.

a loss of 514,000 ETH.[323] In 2022, the decentralised exchange (DEX) OptiFi unwittingly executed a kill switch locking up 660,000 USD Coin.[324] The developer team was attempting to update its Solana program code and triggered the 'Solana program close' function shutting down OptiFi's main network and rendering the lost coins irretrievable. The event, a result of human error also ended up shutting down the exchange.

Terminability exists on a spectrum of prohibition. Other measures also exist along this spectrum. Ocean protocol mentioned throughout this report has a purgatory function to handle IP violations and sensitive data. The 'Ocean Market Purgatory Process' handles the IP violations and sensitive data in Ocean Market.

A public data asset tagged as 'in purgatory' in Ocean Market will have implications for how that data is displayed and what actions may be performed on the asset. Data assets can enter purgatory if there is a formal takedown request for IP violations or sensitive data.

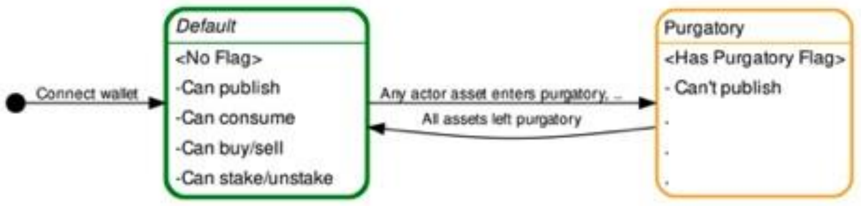
Figure 14: Purgatory for data


Asset created
Default
<No Flag>
-Can discover via browse/search/filter
-Can be bought/sold
-Can be consumed
-Can be staked/unstaked
Asset got a notice or flagged
Retracted
Purgatory
<Has Purgatory Flag>
-Not discoverable
-Access only directly from url
-Non-publishers can unstake
-Users can't stake or buy

Source: Ocean Protocol Technical Paper

When an actor (Ethereum address) is 'in purgatory' it affects how the actor profile is displayed, and what actions it can perform on Ocean Market. Actors enter purgatory if they publish an asset that has been put into purgatory or engage in a so called 'rug pull,' a type of cryptocurrency scam where developers attract investors but disappear before the project is finished; selling their tokens and leaving investors with worthless assets and losses.

Figure 15: Purgatory for an Actor



Source: Ocean Protocol Technical Paper

Concepts like the Ocean Market Purgatory Process are additional means to build-in consumer protection and account for liability regimes without resorting to kill switches proper, which can carry serious trade-offs. Immutability is a contentious subject. In the case

[323] https://www.parity.io/blog/security-alert-2/.
[324] https://cointelegraph.com/news/dex-accidentally-hits-kill-switch-on-mainnet-locking-660-000-usdc-inside.

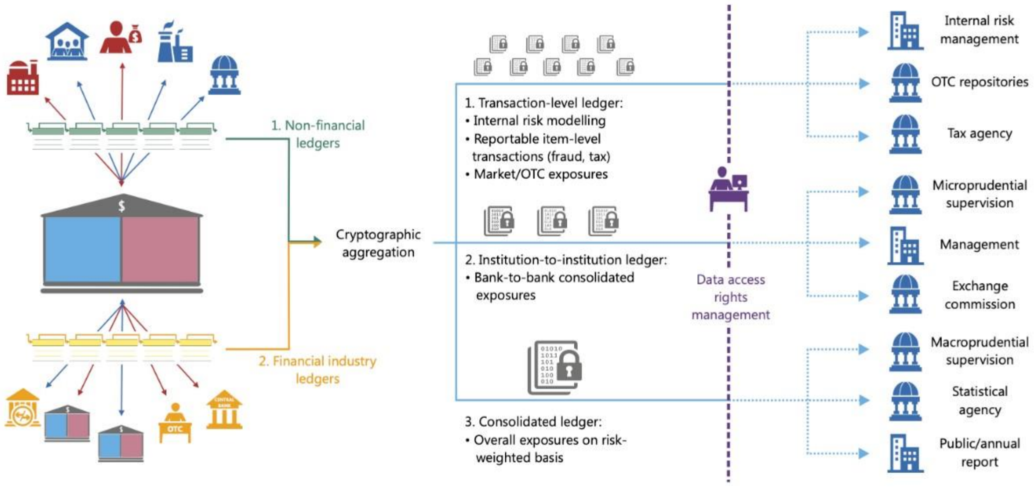
of ‘The DAO’ hack in 2016, those in favour of immutability chose in favour of a hard fork, resulting in Ethereum Classic. Nonetheless, the growth and popularity of Ethereum Classic is dwarfed by the development of Ethereum and the overall EVM ecosystem. Kill switches have merit when considering the need to make quick decisions in times of crises but they also carry penalties (if not implemented correctly) that can lead to more harm than good, undermining their utility. When considering the inherently cross-border nature of smart contracts it poses perhaps the most operational challenges to mandating kill switches. There is also no clear path to understanding what impact such a decision would have on innovation or on the future commercial viability of smart contracts within the Single Market.

3. Embedded Supervision

Embedded supervision is a growing field of interest. The European Commission’s Directorate General for Financial Stability Financial Services and Capital Markets Union (DG FISMA) has recently tendered a ‘Study on Embedded Supervision of Decentralised Finance.’ This pilot project aims to ‘develop, deploy and test a technological solution […] to benefit from the open nature of transaction data on the Ethereum blockchain.’[325] Earlier work by Auer (2019) proposed a set of four guiding principles to govern the use of embedded supervision:[326]

- Embedded supervision needs a regulatory framework with an effective legal system and supporting institutions.
- Markets that achieve economic finality can make use of embedded supervision.
- Economic market consensus matters for how the market may react to automatic supervision in the context of embedded supervision.
- Embedded supervision needs should promote low-cost compliance alongside a level playing field for all firms.

Figure 16: Model embedded supervision framework


1. Non-financial ledgers
Cryptographic aggregation
2. Financial industry ledgers
OTC
1. Transaction-level ledger:
• Internal risk modelling
• Reportable item-level transactions (fraud, tax)
• Market/OTC exposures
2. Institution-to-institution ledger:
• Bank-to-bank consolidated exposures
3. Consolidated ledger:
• Overall exposures on risk-weighted basis
Data access rights management
Internal risk management
OTC repositories
Tax agency
Microprudential supervision
Management
Exchange commission
Macroprudential supervision
Statistical agency
Public/annual report

Source: Auer (2019)

[325] https://etendering.ted.europa.eu/cft/cft-display.html?cftId=12079.

[326] Raphael Auer, Embedded supervision: how to build regulation into decentralised finance. Bank for International Settlements Working Papers No 811, 2019, https://www.bis.org/publ/work811.pdf.

Indeed, one of the benefits of decentralised markets is that blockchains use economic consensus rather than intermediaries to build trust across the distribution of market participants. The ledger does the data verification. By using this feature, embedded supervision could drive down compliance costs by automating data collection. An example would be that Basel III capital standards could be automatically verified for banking institutions holding asset referenced tokens (ARTs) by computing the ownership of the borrowing and lending balances alongside risk weights within relevant distributed ownership ledgers.[327] The model of embedded supervision envisaged by Auer (2019) is one between regulated financial institutions backed by an effective legal system and its supporting institutions. I.e., one where the claims on real assets that are digitally represented are validated by the legal system. It stands to reason that this supervisory authority function is designed to engage with decentralised markets that operate on permissioned ledger versions of public chains. An example could be Aave Arc, the decentralised finance (DeFi) liquidity market incorporating Anti-Money-Laundering (AML) compliance.

By contrast, the European Commission's open tender seems to indicate a desire to explore embedded supervision across the entire Ethereum public blockchain. As there is currently no existing framework for embedded supervision, the governing principles in Auer (2019) can be appraised on their merits.

Fully decentralised finance is currently not in-scope under the Markets-in-Crypto-Assets Regulation (MiCA). In this case, applying embedded supervision to DeFi could be applied to those firms that are 'decentralised in name only' (DINO), for which a litmus test could be applied. That being said, this may incur additional costs on the supervisor and market participants. It may also create a bifurcated taxonomy with arbitrage opportunities.

The concept of certain economic finality is another potential headwind. The International Organisation of Securities Commissions (IOSCO) establishes the Principles for financial market infrastructures (PFMI).[328] Principle 8 establishes the rules for settlement finality defined as "the irrevocable and unconditional transfer of an asset or financial instrument, or the discharge of an obligation by the FMI or its participants in accordance with the terms of the underlying contract."[329] The Committee on Payment and Market Infrastructures (CPMI) has applied guidance of the Principles of Financial Market Infrastructures (PFMI) to stablecoin arrangements.[330] Stablecoins (also Asset Referenced Tokens under MiCA) exhibit properties of a financial market infrastructure through the 'transfer function' built into the smart contract logic. In this view, Principle 8 of the PFMI applies to stablecoin arrangements.[331] Auer (2019) accepts that in cases where a financial market infrastructure built on a blockchain has no central intermediary to guarantee the irrevocable transfer of funds, a competing definition may need to be applied.

To supplant legal finality, certain economic finality is suggested and defined as the point where a transaction can be considered final once it is certain that, from a specific moment,

[327] Ibid.

[328] International Organisation of Securities Commissions (IOSCO), Principles for financial market infrastructures (PFMI), 2012. Available at: https://www.bis.org/cpmi/publ/d101a.pdf

[329] Ibid., IOSCO, Principle 8, Settlement Finality

[330] Committee on Payments and Market Infrastructures , Board of the International Organization of Securities Commissions, Application of the Principles for Financial Market Infrastructures to stablecoin arrangements, 2022. Available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD707.pdf

[331] Ibid, PFMI, Stablecoin Arrangements.

it will never be profitable to undo.[332] This is much easier to achieve in Proof-of-Work consensus because the economic cost of rolling back the ledger virtually excludes any attempts to undo a transaction. With Bitcoin, this cost scales proportionally with the halving rate of Bitcoin block rewards, which require an *n* increase in compute to mine half as many Bitcoins every four years due to increases in mining difficulty. Other consensus mechanisms may face a different challenge. One issue is the concept of probabilistic settlement.

In probabilistic settlement, transaction validation via nodes converges to but never reaches zero. With time slip under certain consensus mechanisms or due to a fork, revocation can occur. Therefore, with probabilistic settlement, although the legal framework (including in the case of a stablecoin arrangement – its own rules) can define the point of legal finality, technical settlement may never be guaranteed with absolute certainty. Conclusiveness of the state of the ledger is proportional to the number of transactions, which get added to it. However, settlement risk implications from a fork also increase concurrently with the number of transactions. Proof-of-Work also faces the nothing at stake problem which occurs when the validating nodes in a protocol can generate and maintain multiple forks at no cost.

The above points take on another dimension when considering the added role of the supervisor in embedded supervision regimes. Compliance is an out-of-market cost that firms incur unwillingly. It should be no different that firms operating in blockchain ecosystems would face the same situation and also the incentive to cheat the system. With the nothing-at-stake problem for example, updating transaction history to cheat supervisory authorities remains an attractive option. As the European Commission’s public tender is also exploring embedded supervision outside of the regulated permissioned context of Auer (2019) this is a significant headwind. With Proof-of-Stake for example, the supervisory authority could mandate a proportional increase in the costs of operating and maintaining validator nodes in a PoS network scheme to disincentivize cheating. The downside of this is that the supervisor may inch towards market participation by inadvertently encouraging a certain organisation of the market structure. In this case, one that would favour those firms that can afford the down payment of compliance at the expense of smaller players.

Finally, the above point could then bring the supervisory authority at odds with encouraging ‘low-cost’ compliance by mandating high barriers to entry. Embedded supervision is an important topic, especially in lieu of the growth of the decentralised finance ecosystem. It needs to be understood in the context of balancing market incentives with compliance need and the impartiality of the supervisory authority. This is admittedly a harder point to accomplish in blockchain ecosystems. The case studies have shown that embedded supervision as an umbrella term does not need to be relegated to decentralised financial markets. The case studies have also shown that embedded supervision in the era of Industry 4.0 impacts the hardware level of the technology stack as well. In systems using a network of connected sensors inputting telemetric data, maintaining the security of the chip infrastructure is just as important as monitoring activity on the application layer.

B. Data portability and decentralised identity

[332] Raphael Auer, Beyond the doomsday economics in” proo-of-work" cryptocurrencies. Bank for International Settlements Working Paper No 765, 2019, available at: https://www.bis.org/publ/work765.pdf

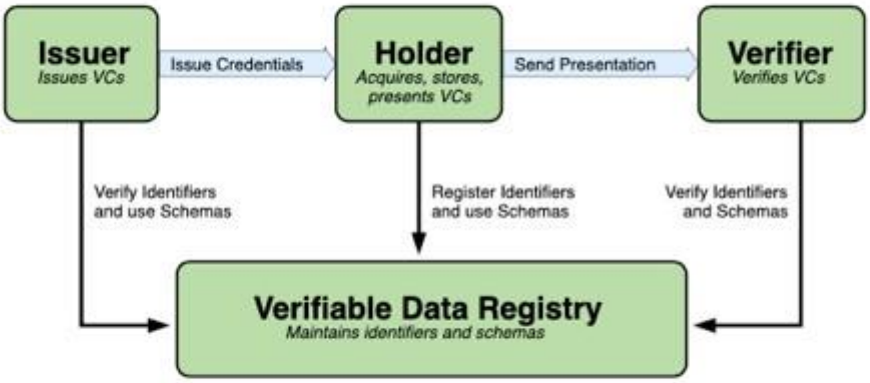
1. W3C Verifiable Credentials

The World Wide Web Consortium (W3C) is the main international standards organisation for the World Wide Web.[333] The standards and interoperability that the W3C promotes include Verifiable Credentials (VC). The W3C has a dedicated working group for the promotion of Verifiable Credential interoperability and best practices.[334]

Verifiable Credentials are tamper-evident credentials that have authorship which can be cryptographically verified. An issuer, which could be an authority on some information about a given subject (e.g., natural person) can issue this information to a holder in the form of a claim. The holder is then responsible for managing and storing the credential. The credential itself often takes the form of software which acts on behalf of the subject (such as a digital wallet). Verifiable Credentials are usually in the form of JSON Web Tokens (JWT) or JSON-LD (JSON-Linked Data).

A verifier can request that the holder of the data needs to meet certain verification requirements when there is a need to validate certain information. Furthermore, the existence of a verifiable data register could be assumed by a system which mediates the creation and verification of identifiers, keys, verifiable credential schemas, revocation registries and issuer public keys.[335]

Figure 17: Actors involved in a Verifiable Credential

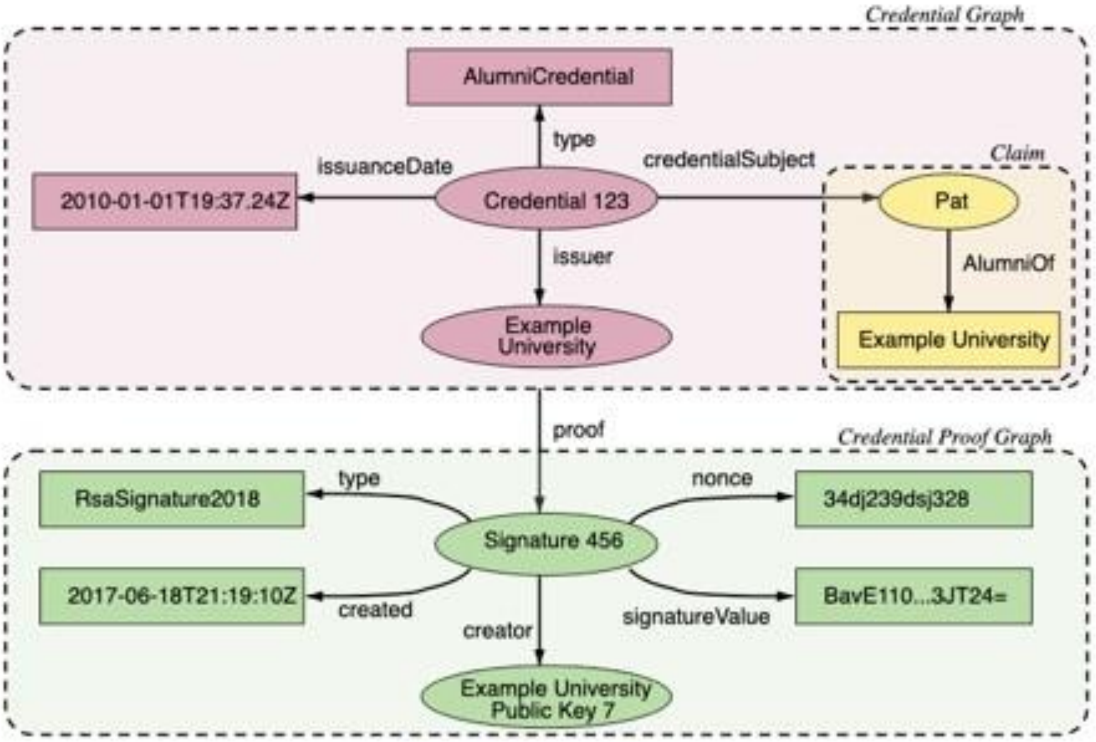

Issuer
Issues VCs
Issue Credentials
Holder
Acquires, stores, presents VCs
Send Presentation
Verifier
Verifies VCs
Verify Identifiers and use Schemas
Register Identifiers and use Schemas
Verify Identifiers and Schemas
Verifiable Data Registry
Maintains identifiers and schemas

Source: W3C

The infographic below shows the main elements of a Verifiable Credential. The first image shows the Verifiable Credential itself complete with both the credential metadata and claims. The second image visualises the digital proof in the form of a digital signature.

[333] https://www.w3.org.
[334] https://www.w3.org/groups/wg/vc.
[335] https://www.w3.org/TR/vc-data-model/.

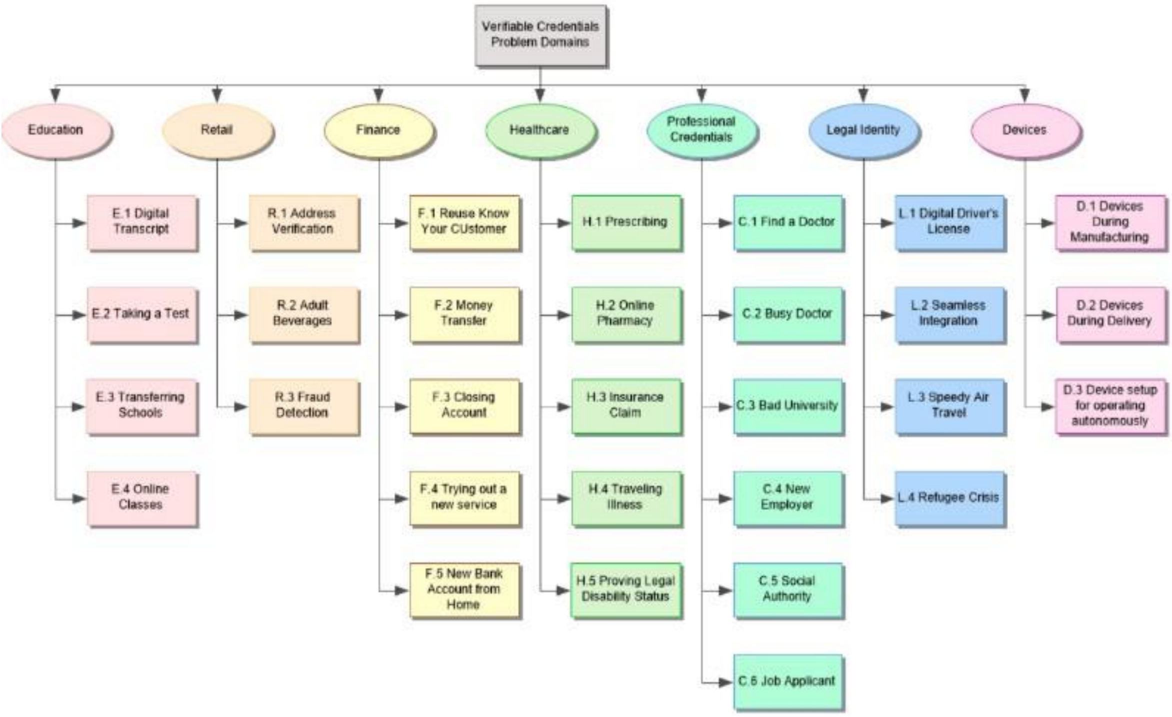
Figure 18: Verifiable Credential process chart



Source: W3C

The ability to partition exactly how much information a holder wishes to reveal can be achieved using any number of technological substrates. This makes Verifiable Credentials a form of attestation management falling under the umbrella of so called ‘Self-Sovereign-Identity.’ Technological systems that uphold Self-Sovereign Identity are a powerful tool for personal data management and ownership. This brings SSI in line with the core principles of the GDPR and draft Data Act. Verifiable Credentials have many benefits. They let users make claims as part of their daily lives, which are increasingly led online. Verifiable Credentials can support things like digital driver’s licenses, university diplomas, payment account access, credit scores, and job applications. A figure describing their different use cases is featured below.

Figure 19: Verifiable Credential use-case ecosystem



Source: W3C

The European Blockchain Services Infrastructure and European Self-Sovereign Identity Framework (ESSIF) have identified several use-cases and data models for Verifiable Credentials. Thes include verifiable IDs for natural persons[336] and a verifiable diploma schema[337] among others. Moreover, in 2021, EBSI launched the first EU cross-border pilot which included two European university alliances and eleven universities to create a 'multi-university pilot.'[338] One of the use cases centred around the distribution of an engineering practice license in Cyprus involving Goldman Solutions and Services Ltd (wallet provider) the Greek Universities network (GUnet), the Deputy Ministry of Research, Innovation and Digital Policy of Cyprus and the Cyprus Technical and Scientific Chamber (ETEK).[339] EBSI provided the blockchain infrastructure support. Another related to the use of EBSI infrastructure, Self-Sovereign Identity and diploma management between FR, GR and RO.[340]

2. SoulBound Tokens

SoulBound Tokens (SBTs) are a very recent addition to the digital identity spectrum. They are non-fungible, non-transferrable and public-verifiable digital tokens. SBTs were originally proposed in 2022 in a working paper by E. Glen Weyl, Puja Ohlhaver and Vitalik Buterin 'Decentralised Society: Finding Web3's Soul.'[341] The paper considers the role of

[336] https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Verifiable+ID+-+Natural+Person.
[337] https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Verifiable+Diploma+Schema.
[338] https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Verifiable+Credentials+Success+Stories.
[339] https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Licence+to+practice.
[340] https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Bachelor+-+Master+Degree.
[341] Weyl, Eric Glen and Ohlhaver, Puja and Buterin, Vitalik, Decentralized Society: Finding Web3's Soul (May 10, 2022). Available at SSRN: https://ssrn.com/abstract=4105763 or http://dx.doi.org/10.2139/ssrn.4105763

SoulBound Tokens within the broader context of a ‘decentralised society.’ Weyl et. al (2022) argue that the ‘web3’ ecosystem has an overreliance on centralised management of custodial wallets. Moreover, that decentralised key management systems are adapted to experienced users. Finally, the lack of a native web3 identity makes todays DeFi ecosystem unable to support activities which are ubiquitous in the real economy (e.g., undercollateralised lending or apartment leases).[342] They highlight further how most NFT artists current rely on centralised platforms such as OpenSea or Twitter for scarcity and initial provenance or that decentralised autonomous organisations wishing to move beyond simple coin-voting are forced to rely on social media profiles for sybil-resistance.[343]

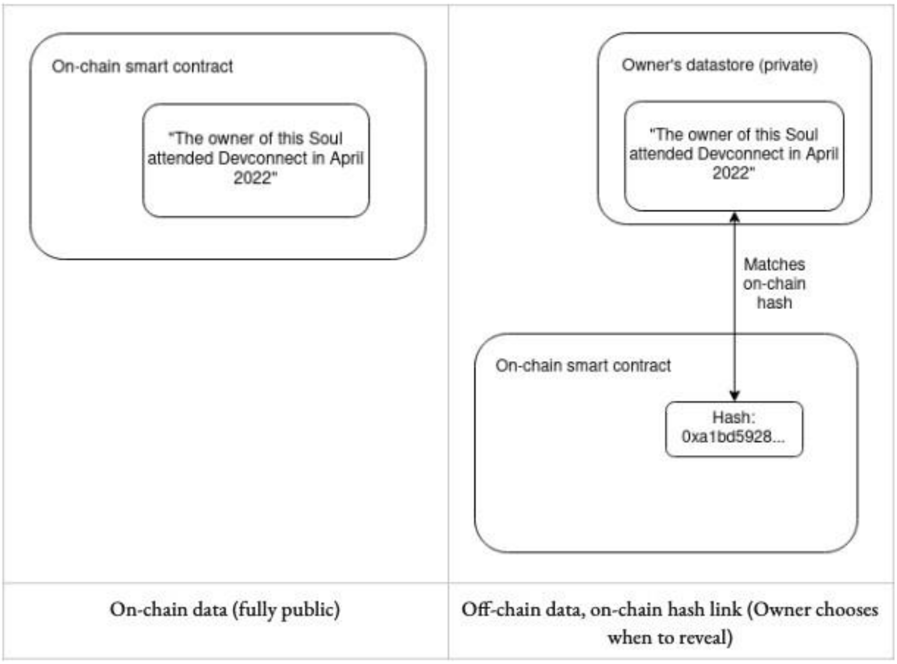
Soulbound Tokens can be applied to any market built on scarcity, authenticity or reputation.[344] Perhaps one of the most interesting applications of SoulBound Tokens is in the domain of property rights. Weyl et. al (2022) argue that ‘innovation will hinge on the ability to decompose property rights to match features of existing property regimes, and code even richer elaborations.’ The list below describes specific applications of SBTs to property rights explained by Weyl et. al (2022):

- Permissioning access to privately or publicly controlled resources (e.g., homes, cars, museums, parks, and virtual equivalents).
- Experiments in market design (e.g., self-assessed licenses sold at auction, SALSA).
- Democratic mechanism design (e.g., quadratic voting schemes).
- Data cooperatives where researchers can use SBTs to grant data access and instantiate access rights. This could be applied to economic benefits borne from intellectual property acquired through research.

The underlying ontology of SoulBound tokens essentially mirrors the traceability of information on blockchains with the ability to also trace social provenance on chain. This makes them suited to deal with manipulations such as deep fakes which artificial intelligence programs are already using to spread misinformation campaigns online.

[342] Ibid.
[343] Ibid.
[344] Ibid.

Figure 20: SoulBound Token utility example


On-chain smart contract
"The owner of this Soul attended Devconnect in April 2022"
Owner's datastore (private)
"The owner of this Soul attended Devconnect in April 2022"
Matches on-chain hash
On-chain smart contract
Hash: 0xa1bd5928...
On-chain data (fully public)
Off-chain data, on-chain hash link (Owner chooses when to reveal)

Source: Weyl et. al (2022)

As mentioned, one of the challenges facing Distributed Autonomous Organisations (DAO) is the over-reliance on things like social media profiles for sybil-resistance. Any one user can accrue multiple wallets, amass tokens and reach the desired 51% of votes needed to overpower the other members. SoulBound Tokens could mitigate sybil attacks in DAOs through targeted 'proof of personhood' SBTs or computing over a holder's constellation of SBTs to screen for bot and unique users, blacklisting any voting power to those users that could be a sybil.[345] SBTs could also deter vampire attacks. In such attacks a DAO free rides on the research and development of another protocol by copying its open-source code and then using a fake token to lure in user liquidity. By encouraging the vesting of SoulBound tokens for those users who are likely to be sybil-resistant, it could also show if any users shifted their liquidity during a vampire attack.[346]

As mentioned, decentralised finance is unable to mirror real world economic utility in the form of undercollateralised lending save in permissioned blockchains where credit professionals can manage the flow of lending to institutional borrowers on the basis of pooled capital.[347] With B2C or even C2C lending this is still not possible. The use of SoulBound tokens could allow users to prove meaningful social provenance and secure a loan. Loans and credit lines could be represented as non-transferable but revocable SBTs, so they are nested amongst a user's other SBTs (as a form of non-seizable reputational collateral) until they are repaid and subsequently burned or replaced with proof of repayment.[348] However, it should be noted that this is also the most contentious application of SoulBound Tokens. Although they could serve as a native identity primitive for the

[345] Ibid.
[346] Ibid.
[347] See for example Maple Finance, https://www.maple.finance.
[348] Ibid.

decentralised internet, there is the real risk they could be used maliciously to create a repository of social credit. Any use of SoulBound Tokens for the purpose of staking social provenance against economic benefit should be carefully discussed in the context of values underscoring a free and democratic society so as not to weaponise the technology.

On chain data storage could be left with the users. There are a number of alternatives from the individual to the aggregate level. At the lower end, storage on their own devices, including inside wallets. On the other hand, storage on the Interplanetary File System or other decentralised networks. There is also the option of using a trust cloud-service provider. On chain data storage allows for smart contracts that permission the right to write SoulBound Token data while also possessing separate read permissions for the data. Zero-Knowledge proofs (discussed in detail in the next section) would allow users to selectively show their data but are also compatible with negative reputation (e.g., credit scores, unpaid loans, negative reviews).[349] The smart contract logic could be designed to include negative SBTs into a Merkel Tree[350] style data structure stored on chain where a zero-knowledge proof would require the disclosure of certain information. This would prevent any gaps in data required for attestation by a verifier in specific cases.

In cases where users lose access to their private keys and their Soul wallets are hacked, Weyl et. al (2022) discuss the possibility of a 'social recovery model' which vests back-up access control of a user's wallet to a set of guardians.[351] Such a social recovery model could also be used for managing access control to update/terminate/govern smart contracts with changes made available pending a pre-defined number of people are approving. This approach mirrors hardware wallet provider Trezor's seed recovery model called 'Shamir Backup' which is the division of a hardware wallet recovery seed among several wallets.[352] Ledger, another well-known wallet provider has recently come under fire for a similar firmware update which allows users to link their seed phrase recovery to a national ID or passport[353]. The firmware update creates three encrypted fragments of the recovery phrase entrusted to custodians (Ledger, Coincover and a third provider). Amidst security concerns from the community, Ledger has since paused 'Ledger Recover' pending accelerated efforts to open source the code, ensuring it is auditable.[354] This illustrates that any form of 'social recovery' or back-up needs to guarantee trust, either in the code or in the people behind the code to be viable and widely adopted.

3. Zero-Knowledge Proofs

Zero-Knowledge Proofs are an important development in computational mathematics and are a subset of what is known as homomorphic encryption. Zero-Knowledge Proofs are cryptographic proofs where verifying the proof is possible without revealing what is being verified. There are three main elements:

- **Witness**: A prover's assumed knowledge of the witness (secret information) generates a set of questions that is only answerable by a party with knowledge of the information.

[349] Ibid.
[350] A Merkel tree or hash tree is a method used in cryptography where each node (leaf) gets labelled with a cryptographic hash of a data block, while every node that is not a 'leaf' gets labelled with a cryptographic hash of the labels of its child nodes. Merkel trees enable the contents of large data structures to be verified securely.
[351] Ibid.
[352] https://trezor.io/learn/a/what-is-shamir-backup
[353] https://www.ledger.com/academy/what-is-ledger-recover
[354] https://cointelegraph.com/news/ledger-recover-paused-code-will-open-source

- **Challenge**: Once the prover has randomly chosen a question and calculated an answer it is set to the verifier who picks another random question from a set, asking the prover to answer it.
- **Response**: The question is accepted, and the answer is calculated before being returned to the verifier. To prevent the chance of a one-off, this sequence can be repeated many times until the prover is satisfied that the witness is not faked.

This form of ZKP is known as an *interactive* proof in that it requires two parties that are both available and can make repeated iterations of the process until a verifier is convinced of a prover's honesty. The proof would still be unavailable for independent verification. Blum et. al (1988) developed the first *non-interactive* zero-knowledge proof. They provided a way for any zero-knowledge proof to be replaced by sharing a common, short, random string to construct a public-key cryptosystem secure against chosen ciphertext attacks.[355] Generated proofs are available for verification to anyone with access to the shared key[356] and verification algorithm. The two types of non-interactive proofs are:

- **Zero-Knowledge Succinct Non-interact Argument of Knowledge (zk-SNARKs):** Verifying the proof is possible without revealing what is being verified and without any interaction between the prover and the verifier.
- **Zero-Knowledge Scalable Transparent Arguments of Knowledge (zk-STARKs):** Users can share either validated data or perform computations with a third-party without revealing the data and/or computation to the third party. STARK proofs are larger, but this gives them higher verification overheads (computation heaviness).

Like other artifacts in the broader decentralised identity ecosystem ZKPs are designed to shield personally identifiable information (PII) from unwanted third parties. The use of ZKPs as a substrate can be combined with other technologies in identity credentials, proving authentication access to certain platforms but also verifiable computation. The latter is a growing use-case for ZKPs also within the broader Ethereum ecosystem. Through verifiable computing, protocols can outsource this part of the value chain to a third party and through ZKPs maintain proof that the computation was executed correctly. This can reduce latency on blockchains without sacrificing on-chain security. In terms of portability, ZKPs have another benefit over more simple Verifiable Credential approaches. In a Verifiable Credential that makes use of ZKPs, the original credential virtually never leaves the Holder's wallet. Only the credential presentation is disclosed to external parties. This presentation is also generated dynamically as needed rather than being the credential itself. This is due to the fact that as a general level of abstraction, the assertion format is not the same as a particular type of digital signature scheme.

Indeed, a common misconception is that ZKP-based credentials represent a new type of Verifiable Credential. ZKPs are an emergent property or substrate of select digital signature schemes which can be represented in different taxonomies of Verifiable Credentials. An example would be in the above section on SoulBound Tokens leveraging non-interactive ZKPs for the purposes of scaling identification but allowing data to be segregated based

[355] Manuel Blum, Paul Feldman and Silvio Micali, 'Non-interactive zero-knowledge and it's applications.' Massachusetts Institute of Technology (MIT) Laboratory for Computer Science, 1988, available at: https://dl.acm.org/doi/pdf/10.1145/62212.62222

[356] Generating the public parameters or Common Reference String relates to the shared key. Creating the CRS is critically tied to protocol security which means the entropy used in generating it can be used to compute false proofs. That is why it is considered a protected activity.

on need. Zero-Knowledge Proofs are continuing to see improvement in scalability because they are also considered increasingly in the context of cross-border payment schemes and user identification. However, their main drawback lies in the fact that they are optimised for a specific type of mathematics. Further, they still require more development to overcome their computation intensity and allow them to be considered in the context of widespread, ubiquitous utility. Even still, encouraging the development of ZKP technology is an important piece of the decentralised identity future. The promotion of the use of ZKP technology in national innovation labs and sandboxes, also with regards to EBSI-level interoperability would be a positive development for Europe.

Conclusion

1. Infrastructure and consumer protection

Applying a wholesale requirement for smart contract termination beyond the scope envisioned in the draft Data Act could create pronounced distortions in the market for public permissionless blockchains. The impact of human error should also be weighed against terminability as recent episodes highlighted in this report have shown. While reverse transactions may help better align smart contracts with the right of withdrawal, mitigate the effects of unfair contract terms or encourage restitution on contact avoidance or termination they are nonetheless prone to deficiencies. Not least of which is the likelihood for new types of fraud and loansharking as described in the case of reversible ERC20/721 contracts (see section A.1 Infrastructure and consumer protection).

As highlighted, certain protocols have means of quarantining assets and sanitizing network activity, stopping short of total shutdowns or ledger rollbacks. However, they are insufficient in the event of code errors or the need to implement a court decision. The use of novel methods such as asset/actor purgatory or inter-protocol black/white listing may be a way to ensure continuity and mitigate risk. Further, the necessity for kill switches in the past has shown that network breaches and hacks are often the result of poor internal governance and risk management. Encouraging the use of multi-signature smart contracts or vote-driven smart contract-based ownership is a way to ensure against the need for kill switches.

Embedded supervision is an important development which could have positive impacts on the safe growth of smart contract use cases in Europe. It would be appropriate to consider the application of embedded supervision within the context of impartiality. If a supervisory authority subscribes to mandating upper limits for guaranteeing economic finality in decentralised networks through validator node minimum buy-ins, it could create barriers to entry and threaten a level playing field for new entrants.

2. Data portability and decentralised identity

W3C Verifiable Credentials, and SoulBound Tokens represent different parts of the decentralised identity spectrum. Zero-Knowledge Proofs can serve as a computational substrate to bridge them and other forms of digital identity. As mentioned in B.1 above, Verifiable Credentials are usually in the form of JSON Web Tokens (JWT) or JSON-LD (JSON-Linked Data). One of the major hurdles is the interoperability barrier between ZKP-based credentials and those built on JWT/JSON-LD credentials. Without a way to easily translate and share the underlying data models between different types of assertion formats, challenges will persist. At a technical level this could include JSON processing with pre-configured '@context definitions.' Although not strictly necessary, it would improve semantic data capabilities. The motivation around the use of ZKPs is centred on privacy, but semantic interoperability is needed for broader utility of Verifiable Credential schemas. To that effect, deltaDAO, along with Polygon and Ocean Protocol is making strides towards semantic interoperability and portability of digital identities across ecosystems within Gaia-X. This is being achieved through a direct bridge to eIDAS Trust Service Providers and 'web3' identities.

Digital identity solutions, both at the level of schema frameworks and wallet services are one area with no clear global front-runner. However, Europe is sup porting the growth of this sector both through the EBSI framework and the European Digital Wallet. Encouraging the development of other schemas such as SoulBound Tokens may also provide a means of user verification and compliance for decentralised finance. The application of SoulBound Tokens which connect to eIDAS Trusted Service Providers and can process data from Trust Anchors could bridge the implementation gap for embedded supervision. It may also provide a native identity primitive for decentralised finance that once applied could lead to safer on-chain activity by improving sybil resistance, guarding against vampire attacks and protecting consumers.

Different types of data (including personal data) will be processed using different types of software and protocols all requiring complex decisions in a quickly changing environment. To the extent that this intersects with the scope of smart contracts under the draft Data Act, there exists a need for those smart contracts to be robust, archiveable, updateable and terminable.

3. Interoperability

Interoperability is a critical question with regards to the future of smart contracts in the EU. What Recital 79 of the Data act makes clear is that 'standardisation and semantic interoperability should play a key role to provide technical solutions to ensure interoperability.'[357] Recital 79 further states that it should befall the Commission to adopt 'common specifications where no harmonised standards exist or where they are insufficient to further enhance interoperability for the common European Data Spaces applications programming interfaces, cloud switching as well as smart contracts.'[358] To that end Recital 79 also enumerates what should be included to achieve semantic interoperability namely reusable data structures and models, ontologies, metadata application profiles, reference data in the form of core vocabularies, taxonomies, code lists, authority tables and thesauri.'[359] Moreover, Recital 80 states the need for a 'presumption of conformity for smart contracts meeting harmonised standards.'[360] Building on this, Article 28 of the Data Act states that such requirements can have a 'generic nature or concern specific sectors'.[361]

Blockchains function based on the rules that govern their protocols and how they reach consensus to verify the accuracy of transactions in a trustless, decentralised way. Blockchain consensus only works natively, so transactions sent outside of a blockchain cannot be verified based on its existing rules. Communication between decentralised applications (dApps) faces the same dilemma. dApps rely on the primary 'layer 1' network for verification, but the shared layer is not able to route transactions between supported dApps. By using relay clients designed for a specific consensus mechanism, one could achieve trustless verification between two blockchains by letting each individual blockchain

[357] Ibid., Data Act.
[358] Ibid., Data Act.
[359] Ibid., Data Act.
[360] Ibid., Data Act.
[361] Ibid., Data Act.

natively verify in the destination chain. This is however again only possible with identical counterparties (two chains, same consensus).

Another common way to overcome the counterparty issue is with trusted blockchain bridges. The simplest form of a trusted bridge is if a user wishes to convert for example, Bitcoin to Ether through a centralised exchange. In practice, the Bitcoin and Ethereum networks are insulated from one another, therefore one needs to trust an intermediary to convert the assets. 'Wrapped' coins are another way to bridge different blockchains requiring external verification. They are also an alternative to exchanges but require trusting a custodian as an intermediary. In practice, one can take an amount of Bitcoin, give it to a custodian[362] to lock it in their 'vault' who then 'mints' or issues the equivalent amount of wrapped Bitcoin (wBTC) in the form of an ERC-20 token that is supported by Ethereum. This wBTC is then fungible across Ethereum-based dApps. To do the reverse, a user would return their wBTC to the custodian who 'unlocks' the Bitcoin they held and returns it.

Other protocols such as Polkadot and Cosmos are working on 'multichain' compatibility. Polkadot achieves cross-chain support through what is known as heterogeneous sharding, which allows customising multiple chains that can undergo parallel data exchange. Polkadot's foundational layer enables consensus, security and supports chain communication for sovereign blockchains with different designs and supported use cases known as Parachains, further supported under a framework known as Substrate. Yet even with Polkadot, multi-chain interoperability is only between its own ecosystem External communication with blockchains outside of its native ecosystem still requires the use of cross-chain bridges. Cosmos achieves cross-chain communication through the Inter-Blockchain Communication Protocol which enables trustless data-transfer between sovereign chains while leveraging the native bridging approach via relays. Verification takes place at the destination chain. Like Polkadot, Cosmos also needs to rely on cross-chain bridges for external communication. In that regard, it stands to reason that what is enumerated under Recital 79 of the Data Act would be easier to achieve within the insular ecosystems of a given blockchain's own consensus mechanism and exceedingly complicated to (safely) achieve outside of it. As mentioned earlier in this report, cross-chain bridge hacks are a single point of failure in blockchain systems because they aggregate a pool of assets and become a beacon for would-be hackers who have a harder time exploiting the native chain but can attack the margins (bridges) instead.

A presumption of conformity in line with the draft Data Act is achieved when the smart contract is aligned with a dedicated hEN (harmonised European Norm). Currently, the European Commission is bringing together ETSI and CEN CENELEC to develop a technical specification in line with the Data Act, also in line with the Annual Work Programme 2022.[363] Outside this there is further work being done to encourage the international standardisation of blockchain technologies through the Blockstand Initiative.[364] The consortia is led by the Digital SME Alliance, Small Business Standards (SBS), UNINFO and the International Association for Trusted Blockchain Applications (INATBA). Over a two-year cycle, Blockstand will generate a standardisation platform and a web-based platform to connect stakeholders and find resources related to blockchain

[362] The custodian could be a centralised platform, or a decentralised architecture (DeFi) enabled through the execution of smart contracts.
[363] https://commission.europa.eu/system/files/2023-01/cwp2022_en.pdf
[364] https://blockstand.eu/blockchain-standardisation-facility-community-tool/

standardisation.[365] Efforts underway to develop European standards are being complemented by a globally oriented approach also driven by industry in addressing the cross-border challenges of blockchain and smart contracts.

[365] https://www.digitalsme.eu/official-launch-of-new-eu-funded-project-blockstand-levelling-up-european-leadership-in-blockchain-standardisation/

3.4. Analysis on personal data management tools based on DLT

This chapter provides a comprehensive analysis of the potential of DLT and smart legal contracts regarding access to and sharing of personal data, specifically in respect of personal data management tools. It focuses specifically on smart legal contracts rather than smart contracts in general. It builds on the comparative legal analysis of civil law rules applicable to smart contracts as well as on the technical analysis above. Whereas the preceding analysis evaluated smart contracts more generally, this section examines a very specific application of smart contracts, namely personal data management tools.

Blockchains combined with smart contracts enable the distributed recording of encrypted data[366], which can generate efficiency gains and create incentive mechanisms that can result in new markets for (personal) data.[367] This could in turn be a driver for data-based innovations in the European Union, including regarding how data is shared between different actors.[368] In this context, some predict that personal data management tools using blockchain-based smart contracts will be vital components to realise the data-sharing objectives under the draft Data Act. Against this backdrop, the overarching objective of this task is to provide guidance to the European Commission as to how personal data management tools using DLT-based smart legal contracts can be used to further the data access and sharing objectives enshrined in EU legislation, in particular in respect of the draft Data Act. It should be noted that this analysis was developed just days after the European Parliament's amendments were adopted on 14 March 2023, thus our analysis is mainly based on the draft Data Act published by the European Commission on 23 February 2023 with some references to the European Parliament's amendments where most pertinent.

The analysis engages in particular with the potential and limitations of personal data management tools, also called Personal Data Management Systems (PIMS) regarding the access to and sharing of personal data. From the outset, it is vital to stress that PIMS are a broad category of technologies that have been defined as 'systems that help individuals to have more control over their personal data'.[369] PIMS are indeed best understood as a class of techno-organisational tools that leverage different combinations of different technical elements to ultimately give their users more transparency and control over their personal data. Smart legal contracts are but one of different possible technical tools that can be used to implement this objective underlying PIMS.

Personal data management tools have long been predicted to be a potentially powerful tool to give data subjects more control over their personal data, for instance in facilitating the exercise of their rights under the European Union's General Data Protection Regulation[370]

[366] Article 2, Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology, COM(2020) 594 final.
[367] Finck M (2019) Blockchain Regulation and Governance in Europe, Cambridge: Cambridge University Press, 136.
[368] European Commission (2017), 'Commission Staff Working Document on the free flow of data and emerging issues of the European Data Economy' SWD, 2 final 13.
[369] European Data Protection Supervisor, Opinion on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data (2016), available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en.
[370] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of personal data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

('GDPR').[371] In the future, the practical significance of personal data management tools could gain an entirely new dimension should the draft Data Act, a proposal for an EU regulation that would create a new legal basis for data-sharing, enter into force.[372]

Indeed, the new access and portability rights foreseen in Articles 3-7 of the draft regulation would benefit from adequate technical tools to achieve its objectives of contributing to greater access to and sharing of data across the European Union. This is so, inter alia, because it requires that citizens take personal initiative if they choose to exercise this new right to informational self-determination, yet experience in EU data protection law so far, such as regarding the right to the portability of personal data under Article 20 GDPR, has shown that individuals only rarely exercise legal portability rights. Technology could lower existing barriers to the exercise of such data rights. Technical tools could render related processes more efficient and transparent in order to lower existing barriers to personal initiative. Whereas this is considered to directly benefit data users and data subjects in giving them more transparency and control over the processing of personal data that relates to them, this would also help achieve the draft Data Act's underlying objectives of increasing access to and sharing of personal data. As such, it is expected to drive data-related innovations and to increase the competitiveness of the EU internal market.

Notwithstanding, at the time of writing of this report, PIMS are still a nascent product category with varying structures, business models and technical backbones. This study focuses on one specific technical element that, importantly, can, but does not have to, be used in personal data management systems, namely smart contracts. Generally, smart contracts allow for transaction engagement between two or multiple parties.

The analysis evaluates the potential of smart legal contracts to facilitate the kind of data exchanges anticipated by the data-sharing regime of the draft Data Act. Indeed, it has been highlighted that there is a need to explore the potential '*for smart contracts to support a competitive and fair data economy by technical protection measures that ensure respect for data rights and contractual conditions for data sharing*'[373], stressing further that smart contracts have an '*untapped potential to facilitate automated data sharing and pooling at scale while enforcing usage restrictions*'.[374] In particular, smart contracts' ability to automatically execute and settle transactions for data could *'enable data holders to program precise conditions for how, when and with whom else the recipient data is shared. Smart contracts linked to crypto digital assets also support escrow solutions that are needed to sanction a breach of conditions for data sharing*.'[375] As a result, smart legal contracts are considered to be a useful technological tool for data sharing between entities that do not trust one another, as is the case in the new data portability regime anticipated by the draft regulation.[376]

We take these assumptions regarding smart legal contracts' usefulness in automated transactions for data as our starting point and evaluate (i) to what extent smart legal

[371] See, by way of example, European Data Protection Supervisor, Opinion on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data (2016), available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en.

[372] The draft Data Act is available at: https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data.

[373] European Commission, Inception Impact Assessment for the Data Act (2021) 3527151, 28 May 2021, page 1.

[374] European Commission, Inception Impact Assessment for the Data Act (2021) 3527151, 28 May 2021, page 3.

[375] Commission Staff Working Document, Impact Assessment Report Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act) COM (2022) 68 final, page 17.

[376] Ibid.

contracts are in fact a useful component of PIMS; and (ii) what legal principles PIMS need to abide by in order to be compliant with EU law.[377] This will then enable us to address the broader underlying question of the present study, namely whether there is a need for a Commission initiative regarding the roll out of PIMS using smart legal contracts union wide.

To achieve these objectives, the analysis is divided as follows. First, we will provide a background to set PIMS and their potential (future) relevance for EU data law and, relatedly, the supranational data economy, in context. Section 3.4.1 will briefly introduce the current ability to exercise informational self-determination and explain the EU legislature's intention to increase the access to and sharing of data, inter alia through the draft Data Act's new data portability mechanism. The draft regulation will be introduced, and we will identify the most pertinent legal questions that arise in relation to PIMS using smart legal contracts, which will then be addressed in the subsequent section. Section 3.4.2 will introduce PIMS and their main features. Based on desk research, as well as interviews with industry, we outline various features of PIMS and examine to what extent smart legal contracts are deemed to be important components thereof, both from a theoretical and practical perspective. Section 3.4.3 subsequently determines what design features compliant PIMS using smart legal contracts would need to respect with reference to the most relevant provisions of the General Data Protection Regulation and the draft Data Act. Finally, Section 3.4.4 determines, on the basis of desk research as well as the outcome of industry interviews, how the design of PIMS using smart legal contracts can account for different interests, particularly as arising between (i) the data holder, the data user and the third party under the draft Data Act; (ii) between the data controller and the data subject under data protection law; and (iii) between the consumer and the trader in consumer protection law, taking into account the findings of the comparative legal and technical analysis above.

3.4.1. The Ability to Exercise Informational Self-Determination in Contemporary Data Ecosystems

This section sets out the background of current debates around PIMS using smart contracts to give individuals more practical/effective control over their data. It starts by briefly charting the ability to exercise informational self-determination in contemporary data ecosystems and then outlines the draft Data Act's attempt to create new data portability mechanism to provide natural persons with more control over the data that they share with others. This new legal tool is ultimately also expected to increase access to and sharing of data in the EU internal market.

Recital 7 of the General Data Protection Regulation ('GDPR') explicitly states that data subjects 'should have control of their own personal data'. This is ensured, amongst others, by data subject rights as laid down in Chapter III. However, the ability to exercise such control might be affected by technical and organizational complexity. Indeed, contemporary technical infrastructures have been shown to oftentimes prevent individuals from understanding what exactly they consent to, how their data is processed and what remedies they may have.[378]

[377] The full assessment of compliance of each PIMS is of course contextual and situational. This study focuses on the most pertinent elements under the draft Data Act as well as data protection law.

[378] Elettra Bietti, Consent as a Free Pass: Platform Power and the Limits of the Informational Turn, (2020) 40 Pace Law Review 307.

Current data ecosystems are oftentimes characterized by unfair conditions and existing legal terms and conditions, in addition to prevailing technical infrastructures, make it difficult for individuals to exercise their rights in relation to such data.[379] This has resulted in a situation where data brokers, AdTech companies and large platforms have ever more granular insights about our online behaviour whereas data subjects lose control over their digital footprint.[380] As Bietti has shown, the processing of personal data is frequently based on the legal ground of consent, yet this has largely become a rubber-stamping exercise as due to the complexity of current data processing methods and ecosystems that has become normatively futile and positively harmful.[381]

Experience in data protection law moreover indicates that individuals rarely exercise the rights they have in relation to their data.[382] Such inertia is due to numerous factors, the so-called 'privacy paradox',[383] but also because data protection rights, such as the right to data portability in Article 20 GDPR "is barely known among consumers and can currently only be implemented in a fragmented manner" in the absence of adequate technical tools.[384]The same inertia adopted by most data subjects vis-à-vis their rights under data protection law could thus also come to be transposed into the draft Data Act's anticipated new portability regime, which would strongly curtail its objective of furthering data access and sharing in the internal market.

Article 20 GDPR was one of the true novelties introduced by the GDPR. While this right has no precedent in supranational data protection law, it gives expression to the Regulation's dual objective of implementing the fundamental right to data protection while at the same time promoting the free flow of personal data in the internal market.[385] The right to the portability of personal data also gives expression to the ideal of informational self-determination, the idea that data subjects should be able to control what happens to their personal data.

The right to personal data portability gives data subjects the right to 'receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format'[386] as well as to 'have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided'.[387] This individual right, however, only applies in a limited set of circumstances, namely (i) where the legal basis for the processing of personal data is consent or contract under Articles 6 and 9(2)(a) GDPR and (ii) the processing is carried out by automated means.[388] It is moreover subject to an important limitation, in that it only

[379] European Data Protection Supervisor, Opinion on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data (2016), available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en, 5.

[380] See further Michael Veale and Frederik Zuiderveen Borgesius, 'Adtech and Real-Time Bidding under European Data Protection Law' (2022) 23 German Law Journal 226.

[381] Elettra Bietti, Consent as a Free Pass: Platform Power and the Limits of the Informational Turn, (2020) 40 Pace Law Review 307.

[382] Theo Bertram et al, Five Years of the Right to be Forgotten CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, November 2019 Pages 959–972, available at: https://doi.org/10.1145/3319535.3354208.

[383] See, by way of example, Barth, S., & De Jong, M. (2017). 'The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review'. Telematics and Informatics. 34 (7) pp. 1038 – 1058. Available at: Doi.org/10.1016/j.tele.2017.04.013.

[384] Sophie Kuebler-Wachendorff, Robert Luzsa, Johann Kranz, Stefan Mager, Emmanuel Syrmoudis, Susanne Mayr & Jens Grossklags, "The Right to Data Portability: conception, status quo, and future directions" (2021) Informatik Spektrum 264.

[385] For a conceptual assessment of this right, see further Orla Lynskey, 'Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability (2017) 6 European Law Journal 793.

[386] Article 20(1) GDPR.

[387] Article 20(1) GDPR.

[388] Article 20(1) GDPR.

covers data that has been 'provided' by the data subject. This formulation leads to the exclusion of inferred data, which will often be the more valuable data.[389]

A further important practical limitation to the right to personal data portability can be found in Article 20(2) GDPR, pursuant to which the 'data subject shall have the right to have the personal data transmitted directly from one controller to another' but only 'where technically feasible'.[390] This presents controllers with an avenue of circumvention as they can structure their data processing operations in a manner making such portability to third parties unfeasible. Beyond, the exercise of the right to personal data portability shall be without prejudice to Article 17 GDPR and not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.[391] More generally, the right in Article 20(1) GDPR shall 'not adversely affect the rights and freedoms of others'.[392]

These are inherently limiting conditions, the uncertain and open-ended formulation of which considerably limits data controllers' incentives to respond positively to a request for portability. What is more, they are particularly limiting in the context of the Internet of Things as controllers will usually not know, and not have control over, which data is being processed by, for instance, a smart speaker or watch.[393] Once under the physical control of its owner, that person can control to what extent others can interact therewith.

As a result of the currently limitations of the ability to exercise informational self-determination, current regulatory proposals such as the draft Data Act and more generally the legislative package on digital law that has been proposed by the Commission seek to revive such control in providing for new legal avenues through which personal and non-personal data can be accessed and controlled.[394] In this context, personal data management tools using smart contracts could function as a potential technical solution that could enable the efficient realization of the right to data protection while, at the same time, advancing technological and economic development through compliant data-sharing in the internal market, very much in line with the new legislative package around data that is currently being negotiated at EU level.[395] This is particularly relevant in the context of the recently enacted Data Governance Act as well as the draft Data Act, which is introduced just below.

3.4.1.1. The draft Data Act and the Control over (Personal) Data

The draft Data Act published on 23 February 2022 forms part of the broader EU digital law package composed of norms that have recently been adopted or are currently being negotiated.[396] Overall, this package seeks to stimulate a competitive data market, open opportunities for data-driven innovation and make data more accessible by creating

[389] See Recital 14 of the draft Data Act.
[390] Article 20(2) GDPR.
[391] Article 20(3) GDPR.
[392] Article 20(4) GDPR.
[393] The European Data Protection Board's recent guidelines on virtual voice assistance provide guidance on to comply with data subject rights in this specific domain. See further European Data Protection Board, Guidelines 02/2021 on virtual voice assistants (2021).
[394] On the distinction between personal and non-personal data, see further Michèle Finck and Frank Pallas, 'Those Who Must Not Be Identified – Distinguishing Personal from Non-Personal Data under the GDPR' (2020) 10 International Data Privacy Law, 11, available at: https://academic.oup.com/idpl/article/10/1/11/5802594?searchresult=1.
[395] See Section 3.4.3 below.
[396] This includes the Data Governance Act, the Digital Services Act, the draft Digital Markets Act, the draft Artificial Intelligence Act and also the draft European Health Data Space Regulation.

horizontally-applicable sector-neutral rules on the access to and use of personal and non-personal data. Through the creation of novel legal mechanisms designed to incentivize data-sharing in the Digital Single Market, the draft Data Act reacts to recent debates about the need to increase the availability of data to stimulate innovation in data-driven products in the EU.[397] The draft Data Act is a harmonized horizontal norm that can be supplemented through additional, sector-specific, rules at a later stage. It is important to stress that since the Data Act had not been finalised at the time of submission of this study, our analysis is based on the Commission draft of the Data Act.

The draft regulation is based on an assumption that existing barriers to data sharing, including a lack of incentives for the voluntary entering into data sharing agreements, legal uncertainty about related rights and obligations, contracting and technical costs as well as contractual imbalances, poor metadata management and the absence of standards, interoperability and common practices prevent an optimal allocation of data to the benefit of society.[398] Based on the assumption that data is a non-rival good, the regulation seeks to depart from the current model whereby a data holder's factual techno-organisational sovereignty over the non-personal data they control implies that they have exclusive use over such data. The ability to process personal data remains governed by the GDPR. Different solutions to realize this objective have indeed been suggested over the past years[399] - including data pools, data cooperatives, data trusts[400] and data exchanges as envisaged in the recently enacted Data Governance Act. Another example is Article 16 of the Digital Content Directive, which, in the event of the termination of the contract, enables consumers to retrieve their data from traders that provide them with digital content and digital services, to then share this data with other traders.[401]

The draft Data Act seeks to change this under-use of personal and non-personal data through different measures. These include (i) measures to allow users of connected devices to gain access to data that is generated by them as well as to share such data with third parties to provide in particular aftermarket of other data-driven services; (ii) measures to rebalance SME's negotiating power by preventing the abuse of contractual imbalances in data sharing contracts; (iii) mechanisms for public sector bodies to access and use data held by the private sector in exceptional circumstances such as public emergencies; and, finally (iv) mechanisms that enable customers to more effectively switch between different cloud-computing providers as well as rules that safeguard against unlawful international non-personal data transfers. The draft Act moreover specifies that the 1996 Database Directive does not apply to data obtained from connected devices and related services.[402]

[397] See further, European Commission, 'Shaping Europe's Digital Future' (2020) available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273.
[398] Recital 2 of the draft Data Act.
[399] OECD 'Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use Across Societies (2019); Josef Drexl et al, Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (2022) Max Planck Institute for Innovation & Competition Research Paper No. 22-05, Teresa Scassa, "Sharing Data in the Platform Economy: A Public Interest Argument for Access to Platform Data 10 UBS Law Review 1017, For an overview, see Nicolo Zingales, Data Collaboratives, Competition Law and the Governance of EU Data Spaces, in I. Kokkoris (ed) Research Handbook in Competition Enforcement (Edward Elgar 2022).
[400] Lilian Edwards, The Problem with Privacy (2004) 18 International Review of Computers and Technology 263, Sylvie Delacroix and Neil Lawrence, "Bottom-Up Data Trusts: Distributing the 'One Size Fits all' Approach to Data Governance, 9 International Data Privacy Law 236.
[401] Article 16 of Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ L 136/1 of 22 May 2019.
[402] Consolidated text: Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases OJ L 077 27.3.1996, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A01996L0009-20190606.

The focus of the present report lies on the first new legal regime proposed by the draft Data Act, which can be found in Articles 3-7 thereof. These provisions create a new legal framework for the mandatory access to and porting of data generated by the Internet of Things ("IoT") in B2C or B2B contexts. If adopted in its current form, the new regulation would introduce harmonised rules for making data generated by the use of connected products and related services available to users thereof as well as third parties that have been authorized by users.

Article 3(1) of the draft Data Act provides that IoT products and related services that fall within its material scope of application shall be designed and manufactured and related services provided 'in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user'.[403]

This obligation would, however, only apply to data generated by IoT devices and excludes data generated by the use of products primarily designed to display, play, record or transmit content (such as personal computers, tablets and smart phones).[404] Moreover, the obligation enshrined in Article 3 of the draft regulation also only applies to manufacturers. Manufacturers are generally data holders in the meaning of the draft Data Act. The legal definition of the data holder implies that only natural or legal persons who either have (i) a right or obligation to make available certain data as well as (in the case of non-personal data) (ii) the ability to make data available 'through the control of the technical design of the product'. Manufacturers of the product would typically exercise this kind of technical control. The literature has however pointed out that manufacturers can structure their data ecosystems so that they do not have an ability to make data available. As a consequence, they would fall outside the scope of the Act.[405] This may turn out to constitute an important limitation to the draft regulation's future impact.

Article 3(2) of the draft Data Act creates an additional informational obligation for data holders in providing that before concluding a contract for the purchase, rent or lease of a product or a related service, the data holder ought to provide the data user in a clear and comprehensive manner with: information about (a) the nature and volume of the data likely to be generated by the use of the product or related service; (b) whether the data is likely to be generated continuously and in real-time; (c) how the user may access those data; (d) whether the manufacturer supplying the product or the service provider providing the related service intends to use the data itself or allow a third party to use the data and, if so, the purposes for which those data will be used; (e) whether the seller, renter or lessor is the data holder and, if not, the identity of the data holder, such as its trading name and the geographical address at which it is established; (f) the means of communication which enable the user to contact the data holder quickly and communicate with that data holder efficiently; (g) how the user may request that the data are shared with a third-party; (h) the user's right to lodge a complaint alleging a violation with a competent authority.[406]

- Section 3.4.3 will evaluate the potential of PIMS using smart legal contracts to implement the two core legal obligations enshrined in Article 3 of the draft Data Act. First, whether they can use useful tools to make data 'by default, easily, securely and, where relevant and appropriate, directly accessible to the user',

[403] Article 3(1) of the draft Data Act.
[404] See Articles 2(2) and Recital 15 of the draft Data Act.
[405] Article 2(6) of the draft Data Act.
[406] Article 3(2) of the draft Data Act.

and, second, whether they can facilitate the provision of information foreseen in Article 3(2) to data users.

Article 4 of the draft Data Act engages with the right of data users to access and use data generated by the use of connected products and related services where data cannot be directly accessed by the users. It establishes the corollary to the obligation in Article 3 in providing that users of such products have a right to access and use data generated by the use of a product or service 'without undue delay, free of charge, and, where applicable, continuously and in real-time'.[407] This shall be done 'on the basis of a simple request through electronic means where technically feasible'.[408]

Data holders are not entitled to require data users to provide information beyond what is necessary 'to verify the quality as a user'.[409] Furthermore, the data holder shall not keep information on the user's requested access to the data beyond what is necessary for the execution of the access request as well as for the security and maintenance of the data infrastructure.[410] Data holders shall not disclose trade secrets unless 'all specific necessary measures are taken to preserve the confidentiality of trade secrets in particular with respect to third parties'.[411] Data users shall moreover not use the data in order to 'develop a product that competes with the product from which the data originate'.[412]

Where the data user does not qualify as a data subject under data protection law, personal data generated by the use of a product or related service shall only be made available by the data holder to the user where there is a valid legal basis under Article 6(1) GDPR and, if relevant, where the conditions of Article 9 GDPR are fulfilled.[413] Non-personal data shall only be used by the data holder 'on the basis of a contractual agreement with the user'[414] and the data holder shall not use such data in order to 'derive insights about the economic situation, assets and production methods of or the use by the user that could undermine the commercial position of the user in the markets in which the user is active'.[415]

- Section 3.4.3 will evaluate the suitability of PIMS using smart legal contracts to facilitate compliance with the legal requirements set out in Article 4 of the draft Data Act. It will, in particular, examine whether PIMS can be helpful technical tools in order to allow users to (A) access data without undue delay, free of charge, and, where applicable, continuously and in real-time on the basis of a simple request through electronic means;[416] (B) allow data users to easily verify their identity vis-à-vis data holders[417]; (C) facilitate data holders' management of user information as required by the draft regulation[418]; (D) document whether there is a valid legal basis to access personal data[419] and (E) enable control of what purpose the data obtained is used for by the data holder.[420]

[407] Article 4(1) of the draft Data Act.
[408] Article 4(1) of the draft Data Act.
[409] Article 4(2) of the draft Data Act.
[410] Article 4(2) of the draft Data Act.
[411] Article 4(3) of the draft Data Act.
[412] Article 4(4) of the draft Data Act.
[413] Article 4(5) of the draft Data Act.
[414] Article 4(6) of the draft Data Act.
[415] Article 4(6) of the draft Data Act.
[416] Article 4(1) of the draft Data Act.
[417] Article 4(2) of the draft Data Act.
[418] Article 4(3) of the draft Data Act.
[419] Article 4(5) of the draft Data Act.
[420] Article 4(6) of the draft Data Act.

Article 5 of the draft Data Act concerns the data user's right to share data with third parties. Users, or parties acting on behalf of them can request that the data holder 'make available the data generated by the use of a product or related service to a third party' without undue delay, free of charge to the user, of the same quality as is available to the data holder and, where applicable, continuously and in real-time.[421]

Undertakings that have been designated as gatekeepers under the draft Digital Markets Act are not eligible to do so.[422] This measure seeks to prevent gatekeepers from increasing the politico-economic power over data. Users or third parties shall, moreover, not be required to provide information beyond what is necessary to verify the quality of a user or third party.[423] Data holders can, furthermore, not keep 'any information on the third party's access to the data requested beyond what is necessary for the sound execution of the third party's access request and for the security and the maintenance of the data infrastructure'.[424] Third parties are prohibited from using evident gaps in the technical infrastructure of the data holder designed to protect the data in order to obtain access to data.[425] Beyond, data holders are prohibited from using non-personal data generated by the use of the product or related service to derive insights about the 'economic situation, assets and production methods of or use by the third party that could undermine the commercial position of the third party on the markets in which the third party is active, unless the third party has consented to such use and has the technical possibility to withdraw that consent at any time'.[426]

Where the data user does not qualify as a data subject under data protection law, personal data generated by the use of a product or related service shall only be made available by the data holder to the user where there is a valid legal basis under Article 6(1) GDPR and, where relevant, the conditions of Article 9 GDPR are fulfilled.[427] The failure of the data holder and third party to agree on arrangements shall moreover not hinder data subjects' exercise of their rights under the GDPR, in particular the right to data portability under Article 20 GDPR.[428] Again, trade secrets may only be disclosed to third parties where 'strictly necessary to fulfil the purpose agreed between the user and the third party and all specific necessary measures agreed between the data holder and the third party are taken by the third party to preserve the confidentiality of the trade secret'.[429] The right to port data under the draft Data Act shall moreover not adversely affect data protection rights of others.[430]

- Section 3.4.3 will examine whether (A) PIMS providers qualify as parties acting on behalf of users to access data from a data holder; (B) whether PIMS can facilitate making data available 'without undue delay, free of charge to the user, of the same quality as is available to the data holder and, where applicable, continuously and in real-time'; (C) help comply with the requirement to not request more data from the user than necessary to identify them; (D) minimize data on data users' or third parties' access to the data; (E) control what purpose the data obtained under the Data Act is used for.

[421] Article 5(1) of the draft Data Act.
[422] Article 5(2) of the draft Data Act.
[423] Article 5(3) of the draft Data Act.
[424] Article 5(3) of the draft Data Act.
[425] Article 5(4) of the draft Data Act.
[426] Article 5(5) of the draft Data Act.
[427] Article 5(6) of the draft Data Act.
[428] Article 5(6) of the draft Data Act.
[429] Article 5(6) of the draft Data Act.
[430] Article 5(9) of the draft Data Act.

Article 6 of the draft Data Act sets out the obligations of third parties that receive data at the request of the user. It provides that third parties shall process the data obtained under the new mechanism 'only for the purposes and under the conditions agreed with the user'[431] as well as 'subject to the rights of the data subject insofar as personal data are concerned'[432] and delete the data when they are no longer necessary for the agreed purpose.[433] Third parties shall moreover not use data to coerce, deceive or manipulate the user, by subverting or impairing their autonomy, decision-making or choices, including by means of a digital interface[434] or to profile[435] natural persons unless it is necessary to provide the service requested by the user[436]; share data with other third parties (in raw, aggregated or derived form), unless this is necessary to provide the service requested by the user[437]; make the data available to gatekeepers in the sense of the Digital Markets Act.[438] Third parties shall, moreover, not use the data they receive to develop products competing with product from which the accessed data originate or share the data with another third party for that purpose[439]; or prevent users, including through contractual commitments, from making the data available to other parties.[440]

- Section 3.4.3 will determine the suitability of PIMS using smart legal contracts to facilitate the implementation of the requirements in Article 6 of the draft Data Act in examining the suitability of PIMS to control compliance with the purpose limitation principle and

Finally, **Article 7 of the draft Data Act** determines the scope of B2C and B2B data sharing obligations. It provides that the mechanism enshrined in Chapter II of the draft Data Act shall not apply to data generated by the use of products or related services that are provided by micro and small enterprises[441] provided that these do not have partner or linked enterprises that do not qualify as such.[442] Furthermore, Article 7(2) of the draft Data Act explicitly provides that virtual assistants fall within the draft Data Act's definition of a product or related service to the extent that these are used to access or control a product or related service.[443]

Chapter II of the draft Data Act would hence establish a new legislative framework for B2C and B2B access to and sharing for data holders of data generated by the use of connected products and related services to better leverage the non-rival nature of data generated by the Internet of Things. The above overview has illustrated that Articles 3-7 of the draft Data Act set out numerous requirements, some of which may be more easily and efficiently achieved by using technical tools than in the absence thereof.

Below, we set out the requirements subject to more detailed analysis below (some of which are repeated across the various specific provisions of Chapter II).

[431] Article 6(1) of the draft Data Act.
[432] Article 6(1) of the draft Data Act.
[433] Article 6(1) of the draft Data Act.
[434] Article 6(2)(a) of the draft Data Act.
[435] Here, the definition of profiling in Article 4(4) GDPR applies.
[436] Article 6(2)(b) of the draft Data Act.
[437] Article 6(2)(c) of the draft Data Act.
[438] Article 6(2)(d) of the draft Data Act.
[439] Article 6(2)(e) of the draft Data Act.
[440] Article 6(2)(f) of the draft Data Act.
[441] As defined in Article 2 of the Annex to Recommendation 2003/361/EC.
[442] Article 7(1) of the draft Data Act.
[443] Article 7(2) of the draft Data Act.

A more general point that must be noted is that the draft Data Act assumes the use of the legal instrument of a contract in order to govern the relationship between data holders, data users and potentially also third parties in respect to non-personal data.[444] This requirement for contractual arrangements to govern the exercise of the rights and obligations foreseen in Chapter II of the draft Data Act has been described as leading to the emergence of a new data private law framework.[445] Indeed, contracts will likely be the chosen instrument to govern the modalities of data access and use between in these bilateral or triangular relationships. Some have criticized the need for contracts in this setting.[446] According to Kerber, the draft Data Act will be 'weak and largely ineffective' due to an insufficient scope of data, lacking technical interoperability, and high transaction costs triggered especially through the need for a contract.[447] Yet, as contracts remain the chosen instrument in the current version of the draft regulation this study will also examine, in addition to the more detailed questions set out above, whether smart contracts can be a useful component of PIMS in order to execute this requirement of contractual form. To this end, we take into account the findings of the comparative legal analysis under section 3.2.

Summing up the above, the present study will determine whether PIMS are suitable tools to facilitate compliance with the following requirements arising under Chapter II of the draft Data Act:

- To facilitate the conclusion of a contract between the data holder and the data user.
- To enable a data user's access to data held by a data holder without undue delay, free of charge, and, where applicable, continuously and in real-time on the basis of a simple request through electronic means;[448]
- To allow data users to easily verify their identity vis-à-vis data holders[449] without transmitting more data from the user than necessary to identify them;[450]
- To facilitate data holders' management of user information as required by the draft regulation;[451]
- To enable control of the purpose for which the data is used;[452]
- To determine whether PIMS providers can qualify as parties acting on behalf of users to access data from a data holder.[453]

3.4.2. Personal Information Management Systems (Using Smart Contracts)

The draft Data Act would hence create a new form of B2C or B2B right to data portability. However, it is important to note that the entire regime under Chapter II of the draft Data Act is dependent on individuals' exercise of agency over their data, i.e. they need to proactively decide to request access to such data either for themselves or third parties.

[444] See, for instance, Recitals 25 and 26 of the draft Data Act.
[445] See further Dirk Staudenmayer, Der Verordnungsvorschlag der Europäischen Kommission zum Datengesetz (2022) EuZW 596.
[446] Josef Drexl et al, position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (2022) Max Planck Institute for Innovation & Competition Research Paper No. 22-05; Louisa Specht-Riemenschneider, 'Data Act – Auf dem (Holz-)Weg zu Mehr Dateninnovation (2022) ZPR, 137.
[447] Wolfgang Kerber, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives (2022), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436.
[448] Article 3(1) and Article 4(1) of the draft Data Act.
[449] Article 4(2) of the draft Data Act.
[450] Article 5(3) of the draft Data Act.
[451] Article 4(3) and 5(3) of the draft Data Act.
[452] Articles 4(6), 5(5) and 6(1) of the draft Data Act.
[453] Article 5(1) of the draft Data Act.

It has been seen above that currently only very few individuals exercise their data rights, something that is conventionally attributed not to a lack of interest but rather due to factual difficulties (of time and expertise) to exercise personal initiative. A similar fate might await the draft Data Act, unless there are stronger incentives for individuals to exercise their rights and better technical interfaces that make it easy for them to do so. As such, it is a bit surprising that the draft Data Act explicitly acknowledges that in data-sharing contexts, technical and organisational measures should be used to protect the fundamental right to data protection.[454] Article 24 GDPR of course already requires that controllers implement appropriate technical and organisational measures to protect personal data. This section incorporates insights from desk research as well as interviews with industry. Personal Information Management Systems are a potentially promising solution to facilitate the exercise of the rights that Chapter II of the draft Data Act attributes to users of IoT devices and related services.

A. Personal Information Management Systems (PIMS)

Personal Information Management Systems have been discussed for a few years now as potential solutions to the difficulties of practically implementing data (protection) rights. The European Data Protection Supervisor ("EDPS") highlighted already in 2016 that there is a need for '*innovative digital tools and business models based on the empowerment of individuals*' to '*allow individuals to benefit from such data-sharing, that is to participate in the use and distribution of their personal information'*.[455]

To this end, the EDPS argued, '*we need practical tools to enable individuals to exercise their rights in a convenient, user-friendly way'*.[456] PIMS were singled out as a tool potentially capable of realizing this potential, which may create a '*paradigm shift in personal data management and processing, with social and economic consequences'*.[457] It is important to note that PIMS are a class of techno-organisational data management tools that include sub-categories such as consent management tools, personal data vaults[458], personal data spaces or personal data stores.[459] Indeed, the definition of PIMS is not yet set in stone. For the purpose of our interviews with industry, we interviewed organisations that self-identify as a personal data management tool or as one provider of a larger PIMS solution.

It is important to stress that PIMS are still at a relatively early stage of development and there is as of yet limited experience regarding their practical use and impact on broader data ecosystems. The core, unifying idea behind these technical tools consists in transforming '*the current provider centric system into a system centred on individuals able to manage and control their online identity'*.[460] This reflects that in principle, '*individuals should be able to decide whether and with whom to share their personal information, for*

[454] Recital 8 of the Draft Data Act.

[455] European Data Protection Supervisor, Opinion on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data (2016), available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en, 5.

[456] Ibid.

[457] Ibid.

[458] https://schluss.org

[459] Yves-Alexandre De Montjoye et al., 'openPDS: Protecting the Privacy of Metadata through Safe Answers' (2014) Plos One, available at: https://doi.org/10.1371/journal.pone.0098790.

[460] European Data Protection Supervisor, Opinion on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data (2016), available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en, 5.

what purposes, for how long, and to keep track of them and decide to take them back when so wished'.[461]

A PIMS is hence a trusted actor that enables its user to handle all their data in a single system, either by exporting all relevant data to the PIMS or by keeping data distributed on different services but using data integration techniques to create a single interface for these sources. The broad category of PIMS has been defined as '*technology-backed mechanisms for individuals to mediate, monitor and control how their data is accessed, used or shared*'.[462] As such, they empower data subjects to exercise more control with regard to their personal data. Indeed, personal data management tools have been qualified as forming part of so-called privacy enhancing technologies ('PET's) as well as forming an approach of privacy self-management.[463] Janssen and Singh have described PETs as typically involving ecosystems, which generally entails a platform, as an intermediary, provides infrastructure and a varying set of tools that users can use for handling their personal data.[464] Within this ecosystem, third parties seek to process user data. To realise these objectives, PIMS employ '*technical, legal and organisational measures that enable users to manage and control their data, and to ensure and validate that the behaviours of third-parties accord with user and platform requirements'*.[465]

It follows that PIMS use technical, legal and organizational measures that equip data subjects with tools to manage their personal data (such as by providing transparency over how and by whom data is processed) and compel third parties to ensure that their personal data processing is in line with the requirements of the platform and the data subject. As such, they stand for a form of data-sharing that is more transparent and more granular than conventional models characterized by opacity and complexity. For example, the German Data Ethics Commission has recommended the use of PIMS regarding the use of data for research, in particular as digital consent management tools in order to enable data subjects to maintain a better overview of their consent practice.[466]

In conclusion, PIMS are hence a nascent and still evolving class of data intermediaries that put a techno-organisational structure at the disposal of data subjects, in order to enable increased transparency and control over data that relates to them.

B. The Main Features of Personal Information Management Systems

There is a relatively large variance concerning business models and technical infrastructure used by personal data management systems. This also extends to the question of whether they make use of smart contracts. Indeed, whereas some PIMS make use of these technologies, others do not. The below overview summarizes the findings we gathered from desk research as well as interviews with industry.

1. Local or Cloud-Based Storage of Data

[461] Ibid.

[462] Heleen Janssen and Jatinder Singh, Personal Information Management Systems (2022) 11 Internet Policy Review, available at: https://policyreview.info/glossary/personal-information-management-systems

[463] Heleen Janssen and Jatinder Singh, Personal Information Management Systems (2022) 11 Internet Policy Review, available at: https://policyreview.info/glossary/personal-information-management-systems

[464] Janssen, H., Cobbe, J., & Singh, J. (2020b). Personal information management systems: A user-centric privacy utopia? *Internet Policy Review*, *9*(4). Available at: https://doi.org/10.14763/2020.4.1536

[465] Heleen Janssen and Jatinder Singh, Personal Information Management Systems (2022) 11 Internet Policy Review, Available at: https://policyreview.info/glossary/personal-information-management-systems

[466] Gutachten der Datenethikkommission (October 2019), p. 126.

Different PIMS have adopted different approaches regarding the question of where the data that they help govern is stored and analysed.

a. Cloud-Based Storage

In cloud-based storage models, the data governed through the PIMS is not kept with the user but rather with the provider, usually in the cloud of a third-party, or potentially also on the servers of the personal data management provider itself. All the data can be kept in a single geographical location, or, alternatively, in various places where a logical link among users' data (which itself may stay with various service providers) would connect the data.[467] Other providers have chosen to store data in a decentralised cloud rather than classical cloud solution.[468]

b. Local Storage

In contrast, in local storage models, the data does not physically move to the PIMS provider but is rather kept on the user's device through storage on devices such as laptops, a smart phones or IoT devices.[469] Regarding the processing of the data by the third party that the data subject grants access to, data is either kept on device and processed there through techniques such as federated machine learning, or, alternatively, exported from the PIMS and moved to the third party for processing. Indeed, depending on the model that is used, data 'either do not leave the PIMS (and in certain models, algorithms are even imported and computed internally) or data are securely transferred to the service providers, where they may also be stored in an encrypted form for the processing operations'.[470] The precise formalities of storage and processing of course determine the amount of control the data user/data subject has over the data.

It is worth noting that hybrids of the above solutions are also possible as some personal data management systems only store data on the end-user's device while also providing backup and storage functionalities that users can chose to use if they so desire.[471] Where users are given a choice between on-device and cloud-based storage they seem to favor the latter for reasons of convenience.[472]

2. Security

The ability to secure the data governed by the personal data management system is, of course, a central factor in generating trust in these services and conversely incentivizing their adoption.[473] Also in this respect, different PIMS make use of different specific solutions.

[467] European Data Protection Supervisor, Opinion on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data (2016), https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en, 6.
[468] Interview with Datafund, Interview with Schuss.
[469] Note that the draft Data Act does not apply to the data generated by all of these devices, as described above.
[470] European Data Protection Supervisor, Opinion on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data (2016), https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en, 6.
[471] Interview with iGrant.io.
[472] Interview with O.Team.
[473] European Data Protection Supervisor, Opinion on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data (2016), https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en, 7.('Security and data protection are the main drivers of PIMS').

In general, cryptography plays a fundamental role in securing PIMS and it is indeed considered a ‘necessary component for the security of the data and for mutual reliance on the authenticity and integrity of data and processing among all stakeholders in the data processing chain’.[474] Encryption is for instance often used to secure the confidentiality of data at rest and in transit and in addition, other cryptographic features can be used in order to ‘verify the authenticity of data to implement user preferences, such as in respect of access rights and duration of storage.[475]

3. Smart Contracts

As part of their variegated technical architectures, some personal data management systems have chosen to make use of blockchain-based smart legal contracts whereas others have not.

Personal data management tools that make use of these technologies have stressed that they present advantages for the self-sovereign management of personal data. It has for instance been argued that regarding the management of health IoT data, blockchain technology “*has multiple compelling features such as chronological and time-stamped data record, auditable and cryptographically sealed information blocks, consensus-based transactions, policy-based access to facilitate data protection, fault tolerant, and distributed ledger*.”[476] Further advantages include the ability to transparently log changes from different geographical sources and that each participant has the ‘*latest data version as ensured by consensus algorithms, and there is confidentiality in each transaction’*.[477]

Blockchains are deemed well-suited for ‘*the implementation of cooperative processes that involve different*[478] *contracts in order to ensure the correct execution of the shared process*.[479] Indeed, smart contracts are considered a valuable component of such systems as they ‘*only accept coded interactions and only if executed by the participants who have the necessary authorizations’*.[480] This can, for instance, be used to verify that only parties authorized by the data subject to process the data indeed process the data.

It is for this reason that blockchain-based PIMS have been suggested as a data management tool in numerous contexts, such as for instance in relation to health information records including ‘mobile health care, environmental records, medical insurance information, family health record, medicine record, public health, genomic medical insurance claims can be stored in a blockchain service on cloud and can be accessed from the authorized persons (…) based on patient’s consent’.[481]

Research has furthermore developed products that use smart contracts based dynamic consent management systems backed by blockchain technology, which ‘*allows users to*

[474] Ibid.

[475] European Data Protection Supervisor, Opinion on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data (2016), https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en, 7.

[476] Pravin Pawar et al, ‘Hitching Medical IoT Devices to Blockchain for Personal Health Information Management’, in Seok-Won Lee et al, Blockchain Technology for IoT Applications’ (Springer 2021) 191, 193.

[477] Pravin Pawar et al, ‘Hitching Medical IoT Devices to Blockchain for Personal Health Information Management’, in Seok-Won Lee et al, Blockchain Technology for IoT Applications’ (Springer 2021) 191, 193.

[478] Luciano Argento et al, ‘ID-Service: A Blockchain-Based Platform to Support Digital-Identity Aware Service Accountability’ 11 Applied Sciences (2021) 165.

[479] Ibid.

[480] Ibid.

[481] Pravin Pawar et al, ‘Hitching Medical IoT Devices to Blockchain for Personal Health Information Management’, in Seok-Won Lee et al, Blockchain Technology for IoT Applications’ (Springer 2021) 191, 193.

control their personal data collection and consent to its usage throughout the data lifecycle'.[482] Here, transaction history and log are recorded on-chain to provide trusted tamper-proof data provenance, accountability and traceability.[483] The concept of dynamic consent is introduced in further detail below.

Some providers use smart contracts. For example, smart contracts can be helpful to realise 'decentralization to achieve independence from any one cloud or storage provider, therefore smart contracts contain the business logic that would otherwise reside at that specific provider'.[484] Others such as MyHealthMyData have used smart contracts to 'manage and authorize data exchange and access, on the basis of user-defined permission/consent settings enforced through dedicated smart contracts' as well as to collect consent.[485] Smart contracts were moreover described as a tool for 'automating control and access to the data, this way securing and allowing auditability of the subsequent processing'.[486]

Beyond, there are providers that currently do not use smart contracts but are considering using them in the future, such as in order to manage consent.[487]Yet, our industry interviews revealed that other PIMS providers do not currently make use of smart contracts. Whereas some offer related functionality, they do not deem that smart contracts are necessary to provide the service that they do.[488] Others have informed us that they do not use these tools as "*smart contracts – along with other blockchain solutions – have major drawbacks from transaction time, to privacy, to security*".[489] Other concerns over the use of smart contracts include the difficulty of designing blockchains that offer privacy as well as the vulnerability of encryption.[490] It has also been pointed out that the use of smart contracts will create security risks.[491] Beyond, it is worth repeating that the technical analysis (section 3.3) has identified that the set-up costs for smart contracts are high, as are the costs of changing these contracts. This may also well add to the reasons why smart contracts are not widely used at this stage.

4. Value-Added Service

According to the European Data Protection Supervisor "*PIMS can be considered intermediaries, or 'platforms' of a sort connecting two sides of the market: individuals offering their data for (re)use on the one hand, and organisations wishing to (re)use this data*'.[492] At their core, PIMS thus provide intermediation services between a data subject and a (prospective) user of that data. In addition to this core functionality, PIMS may also provide additional services.[493] Indeed, '*beyond identification, authorization and privacy*

[482] Mpyana Merlec et al, A Smart Contract-Based Dynamic Consent Management System for Personal Data Usage under GDPR, 21 Sensors (2021), 7994, available online: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8659597/.
[483] Ibid.
[484] Interview with Datafund.
[485] Interview with Lynkeus.
[486] Interview with Lynkeus.
[487] Interview with Schuss.
[488] Interview with iGrant.io.
[489] Interview with O.team.
[490] Interview with O.team.
[491] Interview with Schuss.
[492] European Data Protection Supervisor, Opinion on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data (2016), https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en, 11.
[493] For an overview, see Nicolo Zingales, 'The Rise of 'Infomediaries' and Its Implications for Antitrust' (2019), available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3300688, 21-22.

preferences management, PIMS often provide additional value added services' such as retrieving digital footprint.[494]

These may include profiling services, such as where consumers are provided with insights about their digital footprint that can be inferred from the data they provide, automatic form completion services that enable individuals to facilitate form completion by retrieving relevant information from their personal data stored in the PIMS, certification and verification services that can certify the accuracy of some information provided by the client of the PIMS, such as their identity or information related to their health or financial status; a central digital letterbox that enables users to share information with suppliers (such as making it easier to communicate with customer services) as well as additional controls that help consumers manage and filter the information they share and create personal profiles that they can shared with others.[495]

An important functionality provided by some PIMS is consent management. The data subject's consent is one of the legal grounds on which the processing of personal data can be based[496] and, in some contexts, such as the online provision of services, one of the main grounds that is available for data controllers. It was indeed seen in the introduction that many contemporary data processing practices rely on consent. Yet at the same time, consent is a controversial concept considering its inherent limitations in complex data ecosystems. This is examined in further detail below.

Generally speaking, the precise nature of activities carried out by a PIMS matters in respect of their qualification under EU data law as well as the applicability of related legal duties. For example, PIMS that are determining the means and purposes of personal data processing (which they often will) qualify as data controllers under Article 4(7) GDPR[497] and, depending on their precise activities, personal data management systems will also be data intermediaries under Article 2(11) of the Data Governance Act.[498]

5. Business Models

Different PIMS make use of different business models to ensure the profitability of the services they provide. In its opinion on PIMS, the EDPS pointed out that "it is crucial to ensure the transparency of the business model vis-à-vis the individuals whose data are being processed so that they are aware of the interests at stake (of PIMS and other service providers) and can use PIMS in full awareness"[499] Some personal data management systems use an onboarding fee coupled with a subscription that is tied to a given number of data verifications.[500] In others, the fee for storage and bandwidth used by users is paid directly to the peers providing these services in the decentralized storage network.[501]

[494] European Data Protection Supervisor, Opinion on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data (2016), https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en, 7.

[495] For an overview, see Nicolo Zingales, 'The Rise of 'Infomediaries' and Its Implications for Antitrust' (2019), available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3300688, 21-22.

[496] Article 6(1)(a) GDPR.

[497] European Data Protection Supervisor, Opinion on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data (2016), available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en, 11.

[498] Regulation (EU) 2022/868 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) OJ L 152.

[499] European Data Protection Supervisor, Opinion on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data (2016), available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en, 11.

[500] Interview with iGrant.io.

[501] Interview with Datafund.

C. Limitations and Challenges of PIMS

This section has so far provided an overview of PIMS and outlined their core features as well as their expected benefits. It is, however, also important to point out that while PIMS have been discussed for numerous years, their uptake, as well as data on PIMS, remains limited. This is due to several related limitations.

First, PIMS are and remain a voluntary tool – both for data subjects as well as for entities that wish to process the data. Indeed, a data subject cannot force the data controller to collect its consent through a PIMS. This naturally limits uptake to only those with a self-interest in using the technology. It has indeed been observed that 'PIMS face significant challenges to become mainstream for personal data management in a market dominated by a small number of operators that may often not be interested in creating synergies with them'.[502]

Second, technical interoperability is considered an issue limiting a broader adoption of PIMS. Indeed, in the absence of common technical standards, there is a risk that technical challenges will limit the effectiveness of PIMS as well as of the legal rights under the draft Data Act.[503] It has in fact been stressed that the limited integration with legacy systems hinders a broader proliferation of PIMS.[504] We return to the importance of interoperability below in our recommendations section.

Third, personal data management tools do not single-handedly solve the complexity of data ecosystems and lacking data literacy. Whereas PIMS 'seek to provide users with more information about processing, and may offer some general guidance, it will not always be clear to users what the full implications of certain data processing or transfers are – not least given the risks are often contextual'.[505]

Fourth, by adhering to the individualistic approach to data processing, PIMS ignore the social nature of personal data. Indeed, PIMS will '*likely capture data relating to multiple individuals other than the user – for example, through sensing data from other dwellers or visitors in or around someone's home*'.[506] This is, of course, a broader problem. Indeed, it is worth recalling that neither the draft Data Act nor the GDPR present any mechanisms to deal with this as they are and remain individualistic legal frameworks that rely on personal initiative of one user to, inter alia, facilitate access to and sharing of data.

Fifth, personal data management systems continue to suffer from low usability as it has been stressed that their design and functioning are often still far from being seamless and organic hence limiting their adoption.[507]

[502] European Data Protection Supervisor, Opinion on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data (2016), available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en, 8.

[503] See, generally, Heike Schweitzer and Wolfgang Kerber, "Interoperability in the Digital Economy", Macie Paper Series 2017/02 (2017).

[504] Juan Camilo Vargas, 'Blockchain-Based Consent Manager for GDPR Compliance' in H. Roßnagel et al (eds), Open Identity Summit, Lecture Notes in Informatics, Gesellschaft für Informatik Bonn (2019) 165, available at: https://dl.gi.de/bitstream/handle/20.500.12116/20985/proceedings-14.pdf?sequence=1&isAllowed=y .

[505] Heleen Janssen, Jennifer Cobbe and Jatinder Singh, 'Personal Information Management Systems: A User-Centric Privacy Utopia'? (2021) 9 Internet Policy Review 1, 12.

[506] Ibid,3.

[507] Lachlan Urquhart, Neelima Sailaja, Derek McAuley, 'Realising the Right to Data Portability for the Domestic Internet of Things' (2018) 22 Personal and Ubiquitous Computing 317.

Sixth, it oftentimes remains unclear to users what the benefits of using PIMS are. As such, it has been stressed that there is a need for "more research that explicitly demonstrates the value of use of such technologies and the higher symmetry of power it offers users. This would compel them to adopt such measures into their everyday data interactions, by default".[508]

Seventh and relatedly, control as an end in itself seems unappealing to most citizens and it has been suggested that rather, '*in the long term sustaining shifts away from current business models requires viable use cases where utility and value for end users can be derived from this additional control'*.[509]

Eight, it is unclear whether PIMS necessarily always increase trust in data-sharing. Indeed, it may be that users sometimes would opt to store and process their data with a single, centralized operator as opposed to a personal data management system, which may ultimately make the user feel '*more vulnerable to security threats by placing a big portion of their data in one single location and hence refraining from using it*".[510]

Finally, research has also questioned the extent to which PIMS can '*actually empower individuals and address the concerns inherent in data processing systems*' as they indeed do not address existing asymmetries of power in data ecosystems that are considered a core concern.[511]

3.4.3. Designing Compliant Personal Data Management Tools Based on Smart Contracts

The goal of this section is to establish what design principles PIMS need to respect in order to be compliant with EU law. To this end, we revisit the new data access regime under Articles 3-7 of the draft Data Act as well as the most relevant provisions of the GDPR. Given that the law of personal data protection is not the main focus of the present report, we do not provide a comprehensive analysis of the GDPR and its implication to PIMS. Yet, as the above analysis has unveiled, it is impossible to write about the compliance of systems designed to better manage personal data without also considering data protection law. The draft Data Act would indeed be without prejudice to the fundamental right to data protection and its implementation in the GDPR.[512] This implies that where personal data is ported under Articles 3-8 of the draft Data Act, as would necessarily be the case where PIMS are at play, the GDPR applies in its entirety.

The draft Data Act leaves no doubt that the GDPR applies where personal data is processed under its envisaged portability regime. Indeed, Recital 24 of the draft Data Act provides that "insofar as personal data are processed, the data holder should be a controller" under the GDPR.[513] This legislative definition of controllership is remarkable, as it constitutes a deviation from the general principle that control ought to be determined on the basis of a factual and contextual assessment. It remains to be seen what the implications of this legislative deviation from a generally established principle will be, particularly considering the contested and uncertain nature of the current test of

[508] Ibid.
[509] Ibid.
[510] Ibid.
[511] Heleen Janssen, Jennifer Cobbe and Jatinder Singh, 'Personal Information Management Systems: A User-Centric Privacy Utopia'? (2021) 9 Internet Policy Review 1,3.
[512] Recital 7 of the draft Data Act. See also Article 1(3) of the draft Data Act.
[513] Recital 24 of the draft Data Act.

controllership.[514] Notwithstanding the draft Data Act leaves no doubt that data holders' legal obligations are significantly shaped by data protection law. It is also worth noting that the legislative definition of the data holder as a data controller does not mean that there cannot be additional joint controllers bound by the GDPR.[515] As such, this section returns to some of the crucial elements identified above and will examine in particular the legal grounds of consent and contract, the fundamental principles of transparency and purpose limitation as well as the regime on data subject rights.

The draft Data Act's data access and usage rights of data users and third parties over data held by a data holder could come to constitute a significant paradigm-shift, as indeed today, the data holder's techno-organisational sovereignty over the data in general equals the de facto exclusive use of such data. If successful, the new portability regime would attribute more control to data subjects over their personal data. Yet, as seen above, personal initiative in relation to data has remained limited so far, in part due to lacking technical convenience as well as concrete personal incentives to exercise these rights. The draft regulation's data portability regime also relies on personal initiative to enhance access to and sharing of data as the data user always needs to be at the origin of a request for data, even if a third party is processing the data. It seems questionable that data subjects will be more inclined to exercise personal initiative here as opposed to existing data subjects' rights under the GDPR, unless they are incentivised to do so by concrete benefits and easier technical infrastructures.

This section evaluates the potential of PIMS to realize the following objectives enshrined in the draft Data Act:

- To facilitate the conclusion of a contract between the data holder and the data user.
- To enable a data user's access to data held by a data holder without undue delay, free of charge, and, where applicable, continuously and in real-time on the basis of a simple request through electronic means;[516]
- To allow data users to easily verify their identity vis-à-vis data holders[517] without transmitting more data from the user than necessary to identify them;[518]
- To facilitate data holders' management of user information as required by the draft regulation;[519]
- To enable control of the purpose for which the data is used;[520]
- To determine whether PIMS providers can qualify as parties acting on behalf of users to access data from a data holder.[521]

The need to explore the potential 'for smart contracts to support a competitive and fair data economy by technical protection measures that ensure respect for data rights and contractual conditions for data sharing'[522], has been highlighted, stressing further that smart contracts have an 'untapped potential to facilitate automated data sharing and pooling at scale while enforcing usage restrictions'.[523]

[514] https://academic.oup.com/idpl/article/11/4/333/6355992
[515] See further Article 26 GDPR.
[516] Article 3(1) and Article 4(1) of the draft Data Act.
[517] Article 4(2) of the draft Data Act.
[518] Article 5(3) of the draft Data Act.
[519] Article 4(3) and 5(3) of the draft Data Act.
[520] Articles 4(6), 5(5) and 6(1) of the draft Data Act.
[521] Article 5(1) of the draft Data Act.
[522] European Commission, Inception Impact Assessment for the Data Act (2021) 3527151, 28 May 2021, page 1.
[523] Ibid, page 3.

This section relies on desk research and the findings of our interviews with industry in order to determine whether PIMS using smart contracts are in fact capable of implementing the draft Data Act's goals. It is indeed not unprecedented for smart contracts to be used as an instrument to implement goals set out in EU law. For example, the 2018 Renewable Energy Directive, defines the peer-to-peer trading of renewable energy as 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 or indirectly through a certified third-party market participant, such as an aggregator'.[524] Methodologically, this section returns to the elements of the draft Data Act's portability regime that were introduced above and enquires about the potential of personal data management systems to realize them.

3.4.4. PIMS Using Smart Contracts to Facilitate the Conclusion of a Contract between the Data Holder and the Data User

PIMS using smart contracts have thus been presented as a tool that could facilitate the conclusion of contracts between data holders and data users in order to implement the draft Data Act's data accessibility regime in relation to non-personal data (regarding personal data, processing needs to comply with Article 6(1) GDPR). However, as observed above, the conclusion of a contract through a blockchain-based smart contract risks facing legal challenges in a majority of Member States. In some national jurisdictions, the 'immutability'[525] of the smart contract will be a matter of concern whereas in others the difficulty to assess the character and object of the contract poses a risk to its validity. In consumer contracts, the smart contract will need to enable the possibility of exercising the right to withdraw from the contract within 14 days as well as the execution of the right to suspension. Other general challenges that were identified by the comparative analysis above relate to the implementation of information requirements in B2C contracts as well as questions of competence, the identification of parties to the contract, the assessment of the authenticity and integrity of parties' consent, where appropriate and the interpretation of contractual language.

Table 3 (see section 3.2.7) recaps the challenges identified under the comparative legal analysis. This table recalls that those seeking to use smart contracts to implement the data-sharing objectives of the draft Data Act will be faced with legal uncertainty as well as high legal costs where they attempt to resolve such uncertainty. If the Commission wants to further the use of smart contracts as a means of stimulating the implementation of the draft Data Act's objectives through smart contracts, it could do so through the adoption of model contractual terms as well as interoperability (see further below).

3.4.4.1. PIMS as a Means to Enable Access to Data After a Simple Request Through Electronic Means

Article4(1) of the draft Data Act require that a data user be able to have access to data held by a data holder without undue delay, free of charge, and, where applicable, continuously and in real-time on the basis of a simple request through electronic means.[526] Technical

[524] Article 2(18) of Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (recast) OJ L 328, 82.
[525] On this notion, see further: https://www.minneapolisfed.org/~/media/files/news_events/bank-updates/2019-02/ten-troublesome-blockchain-terms.pdf?la=en
[526] Article 3(1) and Article 4(1) of the draft Data Act.

tools can enable the (at least partial) automation of related data-sharing processes to increase the speed with which data is made available and ensure the continuity of data flows. Some PIMS indeed enable "*flexible access control system which can be moulded to fit whatever standard EU legislators decide*".[527]

At the outset, it is worth noting that there has been academic criticism directed at the language used by the draft Data Act in relation to how, exactly, access to data has to be granted. In its position statement on the draft Data Act, the Max Planck Institute for Innovation and Competition pointed out that the formulation of 'making available of data' in Article 2, read in conjunction with Recital 21, could lead to interpretations that the only obligation for data holders is to enable *in situ* accessibility, i.e. that there is no obligation for data holders to actually transfer any data to data users. This, however, would be a much more limited mechanism than the 'transmitting the data' concept used by Article 5(7) of the draft regulation. To avoid doubt and legal uncertainty and a need for judicial interpretation, this could be usefully clarified by further iterations of the draft Data Act.[528]

First, PIMS could, if legally possible, act as intermediaries for data users to exercise their right to access personal data held by a data holder subject to the conditions set out in the draft Data Act's portability regime. They can similarly assist the exercise of the data subject's right to access their personal data under Articles 15(3) and 20 GDPR. Regarding PIMS as a vehicle for data access under Article 3(1) of the draft Data Act, it remains somewhat unsettled to what degree data users could actually force the data holder to pass through PIMS as an intermediary in order to access the data. This general point concerning the uptake of these tools has already been outlined in our 'limitations' section above. Indeed, Article 3(1) of the draft Data Act provides that products shall be designed and manufactured and related services provided such as that data generated by their use are, inter alia, '*directly accessible to the user*'. This casts some doubt on whether the data user could force the data holder to make their data directly available to a PIMS. Of course, the data user could share related data with a PIMS after receiving it from a data holder. This would, however, impose an additional technical and organizational burden on them, making such initiative less likely.

Second, the draft Data Act's anticipated portability regime will also be an important mechanism for PIMS in that it enables their users to 'populate' these systems with data (in addition to the right to personal data portability foreseen in Article 20 GDPR). Indeed, irrespective of the option of acquiring data through Article 3(1) of the draft Data Act directly through the personal data management system, data users will always have the option of exporting data they receive through this new legal mechanism to the PIMS. As such, the new portability regime would, at least in theory, serve as an additional avenue to augment data-sharing, together with the right to personal data portability in Article 20 GDPR as well as the data subject right to access personal data under Article 15 GDPR. The latter can in fact also be used to populate PIMS with personal data, although with the limitation that there is no explicit requirement that data be provided in a machine-readable format.[529] This again underlines the importance of interoperability, which we return to in the recommendations section below. At the same time, we have stressed the limitations of these existing rights above, namely the lack of adequate technical tools and personal incentives to engage in data sharing, which would also risk playing out in this scenario.

[527] Interview with O.team.

[528] Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data, page 26.

[529] Article 15(3) GDPR.

Third, the draft Data Act's new enhanced right to data portability would enable users to export data to third parties. Pursuant to Article 5(1) of the draft Data Act, users – or a party acting on their behalf – can request that the data holder make available data generated by the use of a product or related service to a third party – which could be the PIMS. The data holder must give way to this request without undue delay and free of charge to the user and provide data of the same quality as is available to the data holder as well as, where applicable (note the practical limitations that can arise due to this formulation) continuously and in real-time. Pursuant to Article 2(7), a third party is a 'recipient' of data[530]that gains access to data at the request of data holder or pursuant to a legal obligation.[531]subjects request that their data be made available to third parties, the same data must be made available in the same manner as if it were made available to data subjects themselves. The latter will be able to act as third parties under Article 5(1) of the draft Data Act.

Considering that this study is concerned in particular with smart contracts, Article 30 of the draft Data Act already envisages that there should be essential requirements regarding smart contracts for data sharing. Several issues have, however, been raised in relation to this provision. First, the provision fails to define what 'data sharing' means. This expression, used in Article 30, is not defined in Article 2 of the draft regulation. Furthermore, debates could emerge as to whether the obligations in Article 30 are limited to "agreements to make data available" that occur within the scope of the draft Data Act or whether it applies to any such agreement.

Second, Article 30 also does not define what a smart contract is and the definition thereof in Article 2(16) has been deleted by the European Parliament's version. Article 30 (ba) of the European Parliament's version implies that only smart legal contracts are included in its scope, yet this needs to be clarified considering the wide-spread misinformation that any smart contract amounts to a legal contract. It would not make sense for simple coded if-then statements to be subject to this legal regime.

Third, Article 30 of the draft Data Act requires 'access controls'. The European Crypto Initiative has highlighted the importance of clarifying that this only applies to access for reading, not modification, which would be impossible to implement.[532] Article 30 also requires that it must be possible to safely terminate smart contracts, yet smart contracts are modular and terminating them will often also negatively influence other applications.[533] These issues need to be clarified and addressed to prevent that a well-intentioned norm ends up stifling innovation in the EU.

[530] Pursuant to Art 2(7) of the draft Data Act, a third party can be a 'recipient' of data: ' 'data recipient' means a legal or natural person, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a product or related service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation implementing Union law'.;

[531] Louisa Specht-Riemenschneider, 'Der Entwurf des Data Act' (2022) Zeitschrift für IT Recht und Recht der Digitalisierung, 816.

[532] https://twitter.com/EuCInitiative/status/1623651807674175490

[533] https://twitter.com/EuCInitiative/status/1623651807674175490

3.4.4.2. PIMS as a Means to Enable Data Users to Easily Verify their Identity and to Facilitate Data Holders' Management of User Information

The practical implementation of articles 4(2) and 5(3) of the draft Data Act requires that data users be able to easily verify their identity vis-à-vis data holders[534] to facilitate data holders' management of user information as required by the draft regulation. In this process, users should not be compelled to transmit more data from the user than necessary to identify them.[535] These requirements intent to make the users' contact with the data holder in the context of the exercise of their portability request as easy and data-sparse as possible in view of facilitating the exercise of this portability right and in compliance with the right to data minimisation under the GDPR. Whereas the data holder 'may require appropriate user identification to verify the user's entitlement to access the data' the information collected should not go beyond this.[536]

PIMS could realise the data-minimised identification of data subjects vis-à-vis data holders (as required by the GDPR) in that these data intermediaries could certify the identity of the data subject towards the data holder without disclosing additional information, such as a copy of a passport. Zero-knowledge proofs or the counterparty identification mechanisms introduced above appear to be a helpful cryptographic tool to realise this objective and should be explored further by research. Similarly, the usefulness of W3C verifiable credentials, discussed in the techno-economic analysis above, should be further studied in the context of PIMS to determine whether they can facilitate data-sharing under the draft Data Act.

PIMS as a Tool to Show the Purpose of Processing

Article 5(1)(b) GDPR requires that the purpose for which personal data is used be specific, explicit and legitimated.[537] This core data protection principles are not affected by the draft Data Act, meaning that purpose limitation must always be safeguarded when personal data is processed. In addition, the draft Data Act also creates additional constraints regarding data usage that are related to the purpose of processing. Whereas Recital 28 of the draft Data Act provides that the user "should be free to use the data for any lawful purpose"[538] third parties are subject to a stricter regime. Indeed, Article 6(1) of the draft Data Act requires that data made available to third parties under Article 5 of the draft Act shall process this data '*only for the purposes and under the conditions agreed with the user, and subject to the rights of the data subject insofar as personal data are concerned, and shall delete the data when they are no longer required for the agreed purpose*".[539] This is an expression of the purpose limitation principle as far as personal data is concerned. Recital 33 confirms that "*third parties to whom data has been made available upon request of the user should only process the data for the purposes agreed with the user and share it with another third party only if this is necessary to provide the service requested by the user.*[540]

In essence, the draft Data Act would thus create a new purpose limitation requirement for non-personal data (where the user enables the processing thereof through a third party)

[534] Article 4(2) of the draft Data Act.
[535] Article 4(3) and 5(3) of the draft Data Act.
[536] Article 5(3) of the draft Data Act.
[537] The principle of purpose limitation is conventionally broken down into the (i) purpose specification, and (ii) compatible use requirements.
[538] Recital 28 of the draft Data Act.
[539] Article 6(1) of the draft Data Act.
[540] Recital 33 of the draft Data Act.

that will exist alongside the general principle of purpose limitation for personal data under Article 8(2) of the Charter of Fundamental Rights (which has been a core tenet of data protection law since its inception). This state of affairs results in different legal obligations for different parties under the draft Data Act.

First, where they qualify as data controllers under the test set out in Article 4(7) GDPR, data holders, data users and third parties need to comply with Article 5(1)(b) GDPR where they process personal data. Specifically, this entails that they need to ensure compliance with the two tenets of purpose limitation under data protection law, namely purpose specification and compatible use.

Second, under Article 6(1) of the draft Data Act, 'the data made available' to third parties can only use the latter 'pursuant to Article 5 only for the purposes and under the conditions agreed with the user'. Regarding personal data, Article 5(1)(b) GDPR must be respected. In practice, the distinction between personal and non-personal data is very difficult to draw in many cases.[541] Whether the purpose limitation test in relation to non-personal data under the draft Data Act is identical to the test that has developed under Article 5(1)(b) GDPR's purpose specification and compatible use requirements may become a topic of contention in the future. However, the current formulation of Article 6(1) of the draft regulation seems to imply that purpose limitation ought to be given the same meaning in both contexts. This is to be welcomed, particularly in light of the difficulty to distinguish between personal and non-personal data in many cases.

Third, data holders are in some cases also subject to engage with the purpose limitation test under the draft regulation. Indeed, Article 5(8) of the draft Data Act mandates that trade secrets shall only be disclosed to third parties to the extent that they are '*strictly necessary to fulfil the purpose agreed between the user and the third party and all specific necessary measures agreed between the data holder and the third party are taken by the third party to preserve the confidentiality of the trade secret*'.[542] This creates an obligation for data holders, namely to determine whether the data protected through a trade secret is necessary for the processing planned by the third party. Furthermore, '*the nature of the data as trade secrets and the measures for preserving the confidentiality shall be specified in the agreement between the data holder and the third party*'.[543]

Fourth, data holders are also liable to comply with purpose limitation in that the draft regulation foresees that they shall not use the obtained data to develop products that competes with the product from which the data originates.[544] Article 4(6) of the draft Data Act indeed includes a purpose limitation: the data holder "*shall not use such [IoT product non-personal] data […] to derive insights about the economic situation, assets and product methods of or the use by the user that could undermine the commercial position of the user in the markets in which the user is active*".

This leaves no doubt that where personal and non-personal data are shared under the new portability mechanism planned by the draft Data Act, the ability to ensure respect for the principle of purpose limitation will be a central component of ensuring overall compliance.

[541] https://academic.oup.com/idpl/article/10/1/11/5802594
[542] Article 5(8) of the draft Data Act.
[543] Article 5(8) of the draft Data Act.
[544] Article 4(4) of the draft Data Act.

Yet, experience with purpose limitation in data protection law leaves little doubt that the principle can be difficult to interpret and implement in practice. [545]

The European Data Protection Supervisor has, moreover, stressed that smart contracts can help make sure that the enforcement of consent and purpose specification are '*automatically verified and enforced, preventing access to the data themselves if rules are not complied with'*.[546] Indeed, PIMS realize this objective in verifying the identity of the data user and match against the permitted purposes. A solution could be that where different purpose the relevant decryption keys become unavailable and prevent access.[547]

Research has, however, also warned that there is no panacea against the fact that generally, user transparency and control diminish as the data moves from one party to another. This also has important implications for purpose limitation. It is indeed important to be aware that once '*data moves beyond a system or organisation's boundaries, the visibility over that data typically diminishes, as does the ability to control any subsequent processing*'.[548] As a consequence, while PIMS can provide users with insights about device-related processing, they '*generally will not (at least at a technical-level) provide users with information about – let alone access to – data that has moved to app developers (and, indeed, beyond)*'.[549] As a consequence, despite using a PIMS, users will generally still have '*little meaningful information regarding the specifics of the data actually being shared between organisations and third parties'*.[550] Beyond, '*if data leave a PIMS in unencrypted form, or even if data are lawfully obtained but subsequently decrypted by an organization that does not comply with its obligations, there is a risk that data will be accessed and used differently from their permitted use configured in the PIMS*.' [551]

This has led to calls for further research about these risks, specifically in the context of the further development of PIMS. Indeed, at present it is considered that there is insufficient discussion about how information can be usefully conveyed as to why 'that particular data is necessary' or 'why these weights are attached to particular data in the analytics process, and, more broadly, why that particular processing needs to occur, and the possible data protection implications this may have'.[552] Indeed, what is considered necessary to better manage the risks inherent to PIMS is 'the ability to actually monitor, track and control data as it moves across technical and administrative boundaries is an area for research'.[553] This could be facilitated by interoperability requirements around purpose limitation, as will be explained in further depth below.

It is worth stressing that although technical solutions to this problem are still imperfect, legal solutions partially address the above-described lack of control over data. This is indeed

[545] See further Asia Biega and Michèle Finck, Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems (2021) Technology and Regulation.
[546] European Data Protection Supervisor, Opinion on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data (2016), https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en, 10.
[547] Ibid.
[548] Heleen Janssen, Jennifer Cobbe and Jatinder Singh, 'Personal Information Management Systems: A User-Centric Privacy Utopia'? (2021) 9 Internet Policy Review 1, 11.
[549] Ibid.
[550] Ibid.
[551] European Data Protection Supervisor, Opinion on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data (2016), https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en, 9.
[552] Heleen Janssen, Jennifer Cobbe and Jatinder Singh, 'Personal Information Management Systems: A User-Centric Privacy Utopia'? (2021) 9 Internet Policy Review 1, 9.
[553] Ibid, 11.

achieved by the purpose limitation principle under data protection law as well as Article 6(2)(c) of the draft Data Act.

PIMS a means to ensure compliance with the GDPR's regime on data subject rights

According to Recital 24 of the draft Data Act: 'Where users are data subjects, data holders should be obliged to provide them access to their data and to make the data available to third parties of the user's choice in accordance with this Regulation.'[554] Where data holders qualify as data controllers, they must abide with the entire catalogue of data subject rights under the GDPR. Article 6(1) of the draft Data Act moreover clarifies in addition to Article 1(3) that third parties shall process the data made available to them pursuant to Article 5 "*only for the purposes and under the conditions agreed with the user, and subject to the rights of the data subject insofar as personal data are concerned*". Indeed, the GDPR applies fully to personal data.

PIMS using smart contracts have been suggested as technical tools capable of facilitating the exercise of data subjects' rights. The transparency that can be afforded by these systems is not just an end in itself but furthermore facilitates data subjects' exercise of their rights, such as the right to access, which is an enabling right for all other data subject rights.[555] Some PIMS using smart contracts have, for instance, been fashioned so as to enable data subjects' right to erasure under Article 17 GDPR as 'using smart contracts, users can request deletion of their data stored off-chain'.[556]

The European Data Protection Supervisor has moreover opined that PIMS are '*among the most promising efforts to implement by design the right to access and rectification and the new right to data portability*.'[557] At the same time, it has however also been highlighted by academic research that thus far, in general, data subject rights have had 'little consideration' in a PIMS context as the focus has mostly lied on providing transparency.[558] Whereas transparency is certainly an enabler of data subject rights, the latter category pursues broader aims in data protection law. In order to remedy the limited reach of PIMS for data subject rights, it has been suggested that they for instance might provide information to data subjects that would help users detail and better target their rights requests.[559]

Transparency

The draft Data Act fundamentally seeks to ensure "*that data holders make data available to data recipients in the Union under fair, reasonable and non-discriminatory terms and in a transparent manner*".[560] This is, for instance, achieved by the mechanism provided for in Article 3(2) of the draft regulation according to which data holders ought to make certain

[554] Recital 24 of the draft Data Act.

[555] Mpyana Merlec et al, A Smart Contract-Based Dynamic Consent Management System for Personal Data Usage under GDPR, 21 Sensors (2021), 7994, available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8659597/ ('transaction history and access log data are recorded on-chain in order to enforce trust and provide tamper-proof data provenance, traceability and accountability').

[556] Mpyana Merlec et al, A Smart Contract-Based Dynamic Consent Management System for Personal Data Usage under GDPR, 21 Sensors (2021), 7994, available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8659597/.

[557] European Data Protection Supervisor, Opinion on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data (2016), available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en, 9.

[558] Heleen Janssen, Jennifer Cobbe and Jatinder Singh, 'Personal Information Management Systems: A User-Centric Privacy Utopia'? (2021) 9 Internet Policy Review 1,8.

[559] Ibid.

[560] Recital 5 of the draft Data Act.

information available to data users. Pursuant to Recital 23, this obligation "*provides transparency over the data generated and enhances the easy access for the user*."[561] It moreover does not affect the data controller's obligation to provide information to the data subject pursuant to Article 12, 13 and 14 GDPR.[562] The draft Data Act also stresses the importance of transparency in the contractual terms agreed between the data holder and the data user for the purposes of data-sharing.[563]

This underlines that transparency is a key principle in EU data law, both when personal data is processed (according to Article 5(1)(a) GDPR as well as, inter alia, under the draft Data Act's portability regime, where it also assumes significance in relation to non-personal data.

The benefits of PIMS for creating more transparency in data processing chains has been stressed time and time again. Indeed, some PIMS using smart contracts enable more transparency as 'transaction history and access log data are recorded on-chain in order to enforce trust and provide tamper-proof data provenance, traceability and accountability.[564] PIMS thus for instance enable data subjects to visualize a history of transactions as well as '*the activities the controller and processor(s) have registered in the network in relation to his data'*.[565] In this system, smart contracts are used to define the logic of the interaction between its participants.[566] More generally, PIMS can help increase transparency in data processing as they can "expose the on-device computations, possibly including the results of those computations, and potentially in a meaningful technical format. This is useful not only for portability considerations (e.g. in a PDS context, potentially moving the results of computations across apps), but also in generally providing users with more knowledge and insight into the nature of data processing occurring'.[567]

To what extent personal data management tools can realize these transparency objectives of course depends on the specific tool in question. Moreover, the European Data Protection Supervisor has called for further research on this issue as to this date, machine-readable expressions of data protection and privacy preferences 'which either travel with the data (often called 'sticky policies') or logically link with the data, and of protocols enabling their exchange has not entered the market yet and needs further investments to break into real-life applications'.[568] It is also worth noting that data transparency should not be considered as an end in itself but rather a means to an end. Among other objectives, transparency indeed helps data controllers comply with their accountability and record-keeping obligations in data protection law[569] as well as data subjects to better exercise their data subject rights under the GDPR.

[561] Recital 23 of the draft Data Act.
[562] Recital 23 of the draft Data Act.
[563] Recital 24 of the draft Data Act.
[564] Mpyana Merlec et al, A Smart Contract-Based Dynamic Consent Management System for Personal Data Usage under GDPR, 21 Sensors (2021), 7994, available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8659597/.
[565] Juan Camilo Vargas, 'Blockchain-Based Consent Manager for GDPR Compliance' in H. Roßnagel et al (eds), Open Identity Summit, Lecture Notes in Informatics, Gesellschaft für Informatik Bonn (2019) 165, available at: https://dl.gi.de/bitstream/handle/20.500.12116/20985/proceedings-14.pdf?sequence=1&isAllowed=y .
[566] Ibid.
[567] Heleen Janssen, Jennifer Cobbe and Jatinder Singh, 'Personal Information Management Systems: A User-Centric Privacy Utopia'? (2021) 9 Internet Policy Review 1,9.
[568] European Data Protection Supervisor, Opinion on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data (2016), available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en, 9.
[569] See, inter alia, Articles 24 and 30 GDPR.

Based on the discussion of the new data access regime under Articles 3-7 of the draft Data Act, as well as of the relevant provisions of the GDPR, several features can be identified, which PIMS using smart contracts need to adhere to in order to be compliant. A check-list for PIMS can be found below.

Compliance Checklist for PIMS based on Blockchains and Smart Legal Contracts

- Ensure that where data is exchanged under the mechanisms foreseen in Articles 3-5 of the draft Data Act, there is a valid contract in place between the data holder and the data user, the user and the data recipient and between the data holder and the data recipient.
- Comply with all GDPR requirements, such as the valid consent, including that it needs to be the data subject providing consent, and the right to be forgotten.
- Periodically match data subject preferences with registered preferences in the PIMS.
- Where the provider of the PIMS qualifies as a third party under the draft Data Act: make sure that data is processed ‘only for the purposes and under the conditions agreed with the user, and subject to the rights of the data subject insofar as personal data are concerned and shall delete the data when they are no longer required for the agreed purpose”.[570]
- Make sure that the data processing being facilitated by PIMS is transparent, the requirements of the GDPR and Art 3(2) of the draft Data Act.

3.4.4.3. Accounting for Different Interests in the Design of Personal Data Management Tools

This section aims to identify how PIMS can be designed to efficiently reconcile different interests of the parties involved in related ecosystems, particularly those of consumers and business users; data subjects and data controllers as well as data holders and data users. These are indeed important considerations for personal data management systems, which, as intermediaries, stand in the middle of these parties and need to account for their respective interests in order to attract their business and ensure legal compliance. This section tracks related obligations and tensions. It takes a more detailed look at supranational consumer protection law and recalls the different design obligations arising from data protection law on the one hand and the draft Data Act on the other. This sub-task closes with the observation that the mitigation of the transaction costs and legal uncertainties regarding the interpretation of certain provisions of the GDPR and draft Data Act that were highlighted above stemming from the existence of different interests for PIMS using smart contracts could be mitigated through increased interoperability between various personal data management solutions as well as the adoption of model contractual terms.

A. Data Subjects and Data Controllers

Data subjects and data controllers generally have competing interests in relation to personal data. At a meta perspective, whereas data subjects will generally want to benefit from a broad interpretation of data protection law’s qualified prohibition of the processing of personal data, data controllers have an interest in processing the personal data in

[570] Article 6(1) of the draft Data Act.

question. These opposing interests also find expression when it comes to the implementation of those elements of data protection law that were pinpointed as being most pertinent for the present report. These are important considerations as some stakeholders have indeed highlighted that of all requirements and expectations, the most demanding challenge for PIMS is the balancing act between the protection of the data controller's corporate interests and consumer respectively data subject rights.[571] The prospect of high fines under data protection law is mentioned as an important element in this respect.[572]

For instance, the transparency requirement arising under data protection law requires the provision of transparency for the data subject; yet at the same time data controllers will have incentives to not make all of their operations transparent and, moreover, legal obligations to protect the personal data of other data subjects. This underlines the importance of clear guidance as to what degree of transparency is required. Another example would be purpose limitation, where the data controller naturally has an interest in a broad definition so as to maintain flexibility regarding its use of the data, yet the fundamental rights perspective indicates that the data subject's interest is in restrictive processing such as to minimize the risks where personal data is processed. Below, it is suggested that technical solutions to this conundrum should be identified through interoperability standards and legal solutions can be defined in the form of model contractual clauses.

B. Data Users vs Data Holders

Today, the data holder's techno-organisational sovereignty over data in general equals the de facto exclusive use of such data. This underlines the existence of asymmetries of control and power over data that is necessarily co-generated by at least two different parties, the data holder and the data user. The draft Data Act's new portability right aims to enhance access to and sharing of data within the Digital Single Market. Yet, these technical and economic considerations as well as the elements outlined above highlight that data holders and data users do not naturally have a shared interest and purpose in the further processing of personal and non-personal data beyond the operation of the IoT product and related services.

Indeed, in general, the data holder may have incentives to favor a restrictive access regime to data as they generally do not benefit from the processing of data by others and have to deal with related transaction costs. In contrast, the data user can be presumed to only exercise their rights under the draft Data Act's portability regime if they indeed have an independent interest in such processing. As a consequence, whenever data users do make use of this right they will benefit from a broad interpretation of the legal provisions in Articles 3-7 of the draft Data Act whereas data holders have an interest in a restrictive interpretation thereof, and they will also have incentives to design their technical infrastructures in a manner that is prohibitive of broad data access, such as in not directly enabling direct access by the user to the data but only providing for indirect access, which indeed would be possible under Article 4(1) of the draft Data Act.[573] Indeed, there remains uncertainty as to how the verb 'shall' in Article 3(1) of the draft Data Act ought to be interpreted, particularly

[571] https://igrant.io/papers/iGrant.io_Managing_Consent_in_a_Data_Sharing_Economy.pdf, page 6.
[572] Ibid.
[573] This provision reads as follows: "Where data cannot be directly accessed by the user from the product, the data holder shall make available to the user the data generated by its use of a product or related service without undue delay, free of charge and, where applicable, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible".

in light of the fact that Article 4 of the draft regulation recognises that not all IoT products and related services will build in a manner that enables data access by default.

Recital 21 of the draft Data Act leaves a lot of room for flexible interpretation by data holders in this respect in stating that data holders may design their products "*to make certain data directly available from an on-device data storage or from a remote server to which the data are communicated. Access to the on-device data storage may be enabled via cable-based or wireless local area networks connected to a publicly available electronic communications service or a mobile network. The server may be the manufacturer's own local server capacity or that of a third party or a cloud service provider who functions as data holder. They may be designed to permit the user or a third party to process the data on the product or on a computing instance of the manufacturer*".[574] This has been criticised as this formulation may be interpreted to indicate that "*this concept only involves an obligation to grant access to the data in the form of in situ accessibility, whether the user should also be allowed to port the data or whether there is even an obligation to transfer the data*".[575] This raises the question of whether there is actually any obligation for the data holder to transmit the data in question. In brief, this formulation, if kept in the final version of the draft Data Act, may undermine the very success of the portability regime as it cannot "*guarantee that the rights can be exercised effectively, mere in situ accessibility may often not be enough*".[576] Interoperability has been suggested as a way to remedy this as the Max Planck Institute for Innovation and Competition's position statement on the draft Data Act indeed calls on the EU legislature "*to consider introduction of specific requirements of holders of IoT data to promote interoperability*" and insert a related provision in Chapter VIII of the draft Data Act.[577]

In order to increase legal certainty and avoid the competing interests of data holders and users from stifling the draft Data Act's anticipated portability regime we recommend the adoption of model contractual clauses and interoperability initiatives, as outlined in further detail below.

C. Conclusions

Our analysis has examined the relation between PIMS based on smart contracts using blockchain technology to some elements of data protection law, the draft Data Act, and consumer protection law. Throughout this analysis, it has become clear that two sets of initiative could reduce transaction costs and, to a lesser degree, increase legal certainty for PIMS in order to make their operation more straightforward, and conversely, facilitate their role in the broader data-sharing framework envisaged by supranational data law: interoperability on the one hand and model contractual clauses on the other. Indeed, model contract terms, as envisaged by Article 34 of the draft Data Act, could be useful for smaller market players in view of reducing transaction costs and providing them with contractual clauses that have been legally vetted to reduce legal uncertainties associated with their operation. These conclusions have also been echoed by industry interviews. This section introduces both mechanisms in turn and recalls their utility to address the action points identified in the previous part of the analysis. This also builds on the comparative legal analysis, which has identified areas of lacking legal certainty that can discourage the

[574] Recital 21 of the draft Data Act.
[575] Josef Drexl et al, Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (2022) Max Planck Institute for Innovation & Competition Research Paper No. 22-05, 26.
[576] Ibid.
[577] Ibid.

adoption of smart contracts as well as the economic analysis, which has shown that the set-up costs for smart contracts are high, as are the costs of changing these contracts. Interoperability and model contractual terms appear promising to address both areas of concern.

Interoperability

Interoperability is "*a technical mechanism for computing systems to work together – even if they are from competing firms*".[578] Data processing systems need to be interoperable for the data access and sharing objectives inherent to the draft Data Act to materialize. By definition, the portability regime in Articles 3-7 of the draft regulation requires that the same data points can be usefully processed across the IT systems of different companies, including PIMS where these function as intermediaries.

The creation of technical standards enabling interoperability is more generally an important element of the European Commission's digital strategy.[579] This reflects that when it comes to data policy, "*law is necessary, but not sufficient. It needs to be supplemented by other policy instruments, fashioned and implemented within a policy network*.[580]" According to Lynskey, subjective rights to control over personal data must be complemented by "an architecture which bolsters individual control over personal data in order to deliver 'partial privacy self-management'.[581] This is also acknowledged by legislators elsewhere. For example, the California Consumer Privacy Act provides the possibility for consumers to communicate their online preferences via technical specification signals.[582]

It is in this context that Articles 28-30 of the draft Data Act create special interoperability requirements for operators of data spaces; providers of data processing services as well as vendors of smart contracts. Whereas interoperability is important more generally for PIMS, the draft Data Act also encourages interoperability in relation to smart contracts specifically. Pursuant to the draft Data Act, it may be '*necessary to lay down essential requirements for smart contracts for professionals who create smart contracts for others or integrate such smart contracts in applications that support the implementation of agreements for sharing data'*.[583] The conformity of smart contracts with those essential requirements could be facilitated by providing a presumption of conformity for smart contracts that meet harmonised standards or parts thereof in accordance with Regulation 1025/2012.[584] In this context, mention should be made of ongoing standardisation efforts in this domain. For example, ETSI PDL11 "Specification of Requirements for Smart Contracts' Architecture and Security", is an important industry specification which aims to provide an overview on developing secure, robust and trusted smart contracts. It is being used as a basis on the further collaborative work of CEN

[578] Ian Brown, "Interoperability as a Tool for Competition Regulation" (2020) OpenForum Academy, available at: https://openforumeurope.org/wp-content/uploads/2020/11/Ian_Brown_Interoperability_for_competition_regulation.pdf p. 5.

[579] See Communication from the Commission, An EU Strategy on Standardisation: Setting global standards in support of a resilient, green and digital EU single market, COM(2022) 31 final.

[580] Bennett, Colin, and Deirdre K. Mulligan 'The Governance of Privacy Through Codes of Conduct: International Lessons for US Privacy Policy' (2012) Available at SSRN 2230369.

[581] Lynskey, Orla, *The foundations of EU data protection law* (Oxford University Press, 2015) 257.

[582] California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100]; Human, S., Pandit, H., Morel, V., Santos, C., Degeling, M., Rossi, A., Botes, W., Jesus, V., & Kamara, I. (Accepted/In press). *Data Protection and Consenting Communication Mechanisms: Current Open Proposals and Challenges*. Paper presented at 2022 International Workshop on Privacy Engineering, Genoa, Italy.

[583] Recital 80 of the draft Data Act. The Commission's proposal for the draft Data Act contained the formulation 'it is necessary', which has been revised to 'it may be necessary' by the European Parliament's version adopted on 14 March 2023.

[584] Recitals 80 and 86 of the draft Data Act.

CENELEC and ETSI to set up a joint technical body which, following the adoption of the Data Act, plans to develop technical specifications in line with the Art. 30.

The draft Data Act moreover stresses that standardisation and semantic interoperability should play a key role to provide technical solutions to ensure interoperability[585] and that it will be necessary to provide presumptions of conformity for interoperability solutions that meet harmonised standards or parts thereof in accordance with Regulation 1025/2012.[586] It anticipates that the Commission adopts common specifications in areas where no harmonised standards exist or where they are insufficient to further enhance interoperability for the common European data spaces, application programming interfaces, cloud switching as well as smart contracts.[587] The draft Data Act also envisages that it may be necessary to adopt specifications for specific sectors.[588] At present, the draft Data Act does not envisage interoperability plans for the portability regime under Chapter II of the draft regulation.[589] Yet, it has been stressed by research that the "*effective exercise of the right of Article 4(1) will critically depend on the form in which the data will be made available and whether interoperability will be enabled. In this regard, it has already been explained that the conditions for enabling the accessibility and usability of the data in technical regards need to be improved by additional requirements*".[590] Research has confirmed that, more generally beyond the draft Data Act, lacking interoperability currently constitutes a factor hindering the implementation of PIMS as the lacking consistency '*in data formats used is a barrier that contributes considerably to the successful implementation of data portability measures*'.[591] Indeed, the success of the draft Data Act's novel portability regime as well as the supporting role of PIMS (using smart contracts) can only be achieved if the data retrieved from one entity is in a form that can be used by another. To date, '*organisational differences in coding styles mean that this situation is not often achieved by default. For an average user, this would pose a hindrance in the porting process with no means to input data in the form the receiver expects'*.[592]

The importance of interoperability and certification for PIMS have also been stressed by expert bodies that have studied personal data management systems in detail, such as the German Data Ethics Commission[593] and federal consumer protection authority.[594] Similarly, the European Data Protection Supervisor stressed the importance of interoperability and

[585] Recital 79 of the draft Data Act.

[586] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance, OJ L 316, 14.11.2012, p. 12–33

[587] Recital 79 of the draft Data Act. See also Article 28 of the draft Data Act.

[588] Recital 79 of the draft Data Act.

[589] It has been considered regrettable that Chapter VIII on interoperability does not "contain obligations of data holders as regards objective requirements for interoperability". Josef Drexl et al, Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (2022) Max Planck Institute for Innovation & Competition Research Paper No. 22-05, 27.

[590] Josef Drexl et al, Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (2022) Max Planck Institute for Innovation & Competition Research Paper No. 22-05, 33.

[591] Lachlan Urquhart, Neelima Sailaja, Derek McAuley, 'Realising the Right to Data Portability for the Domestic Internet of Things' (2018) 22 Personal and Ubiquitous Computing 317.

[592] Ibid.

[593] Gutachten der Datenethikkommission (October 2019), p. 133.

[594] Verbraucherzentrale Bundesverband, 'Anforderungen des vzbv an 'Personal Information Management Systems" (PIMS) und Datentreuhänder (2020), 8.

standardization for personal data management tools.[595] Indeed, the current lack of technical interoperability has been highlighted as a factor limiting broader adoption of PIMS. Indeed, the technical report on Trust Anchors SO/TR 23644 Blockchain and distributed ledger technologies is a step in this direction.[596]
Research has indeed warned that in the absence of common technical standards, there is a risk that technical challenges will limit the effectiveness of PIMS as well as of the legal rights under the draft Data Act.[597] It has, moreover, been pointed out that the limited integration with legacy systems hinders a broader proliferation of PIMS.[598] More generally, it has also been highlighted that personal data management systems continue to suffer from low usability as it has been stressed that their design and functioning are often still far from being seamless and organic hence limiting their adoption.[599] Also this aspect could be addressed by interoperability.

The results of our study confirm that interoperability and common standards would be important for the future developments of PIMS using smart contracts. Industry interviews have confirmed that data interoperability is a core tenet of PIMS.[600] It was for instance stated that "PIMS, in the form of personal data storage, is the "lowest" layer data, in the sense that data from personal storage will get aggregated or combined to higher layers that might call themselves data unions or similar, forming the European data spaces. If the PIMS agree on a common language (or how the translation should occur), that will facilitate easier flow of data to higher levels. Additionally, it will allow individuals to more easily change who can access and use the data, as data will not be locked at any one provider. Therefore, the role of PIMS is crucial in that respect".[601] Interviewees have equally warned that without interoperability, the draft Data Act would be an 'empty gun' devoid of practical effect.[602]

This reflects that basic interoperability between systems helps different actors to share data. Interoperability would furthermore be helpful in relation to other elements identified throughout this study. This includes the creation of tools facilitating compliance with the purpose limitation principles under Article 5(1)(b) GDPR.

Article 30 of the draft Data Act already envisages that there should be essential requirements regarding smart contracts for data sharing. It requires that the vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of an agreement to make data available has to ensure that smart contracts are robust, that they ensure safe termination and interruption, data archiving and continuity as well as access control.[603] They shall, moreover, perform a conformity assessment with a view to

[595] European Data Protection Supervisor, Opinion on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data (2016), available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en, 10.
[596] technical report on Trust Anchors SO/TR 23644
Blockchain and distributed ledger technologies (DLTs) — Overview of trust anchors for DLT-based identity management and currently under development ISO/AWI TS 23516 Blockchain and Distributed Ledger Technology — Interoperability Framework (prepared by TC307 WG7)
[597] See, generally, Heike Schweitzer and Wolfgang Kerber, "Interoperability in the Digital Economy", Macie Paper Series 2017/02 (2017).
[598] Juan Camilo Vargas, 'Blockchain-Based Consent Manager for GDPR Compliance' in H. Roßnagel et al (eds), Open Identity Summit, Lecture Notes in Informatics, Gesellschaft für Informatik Bonn (2019) 165, available at :https://dl.gi.de/bitstream/handle/20.500.12116/20985/proceedings-14.pdf?sequence=1&isAllowed=y .
[599] Lachlan Urquhart, Neelima Sailaja, Derek McAuley, 'Realising the Right to Data Portability for the Domestic Internet of Things' (2018) 22 Personal and Ubiquitous Computing 317.
[600] Interview with O.Team.
[601] Interview with Datafund.
[602] Interview with Lynkeus.
[603] Article 30(1) of the draft Data Act.

fulfilling these essential requirements and, on the fulfilment of the requirements, issue an EU declaration of conformity.[604] Beyond, smart contracts that meet harmonised standards or relevant parts thereof drawn up and published in the Official Journal of the European Union shall be presumed to be in conformity with the essential requirements under Article 30(1) of the draft Data Act[605] and the European Commission may request one or more European standardisation organisations to draft harmonised standards that satisfy the essential conditions under Article 30(1) of the draft Data Act[606] or adopt common specifications by way of an implementing act.[607] The Max Planck Institute for Innovation and Competition has moreover recommended that smart contracts "need tailored solutions to match their technological interoperability specificities. This is vital for properly addressing the role of DLT for making data sharing more feasible".[608] In this context, it is worth noting that, as already highlighted above, there is already standardisation work in this area. CEN CENELEC and ETSI have responded to the call for the Action Grant by the European Commission and plan to set up a joint technical body to develop technical specifications and other standardisation deliverables for smart contracts which would provide a basis for developing harmonised European standards to provide the presumption of conformity with requirements of the Data Act.

Some have cautioned that in the context of the Data Act, interoperability should not be limited to smart contracts but that all data sharing contracts would 'benefit from interoperability and minimum requirements'.[609] Industry organisations have started working on proposals for standardisation efforts and warned that timing is key. On the one hand, such efforts should not come too late as this would slow early investments and possibly also overall market development. On the other hand, such efforts should not come too early as they might then be difficult to implement.[610]

Given the plurality of voices advocating for interoperability in relation to smart contracts on the one hand and PIMS in general on the other, it is evident that interoperability will increasingly be discussed in these contexts in the coming years. In this context, it is also important to be aware of the fact that interoperability is not a zero-sum game. Our techno-economic analysis above has highlighted that blockchain consensus only works natively, meaning that transactions can only be verified where the same consensus mechanism is used between two chains (see analysis further above). Any interoperability standards hence need to be carefully crafted in order to prevent that they stifle nascent innovation towards data-sharing and beyond in the internal market and put the EU at a disadvantage vis-à-vis jurisdictions with better suited legal frameworks.

It is also vital to recall that this analysis has examined smart legal contracts, not smart contracts in general.[611] Interoperability should also be limited to the former as regulating any programmable lines of code (if x then y statements) that automatically executing such actions as initiation, verification, execution and enforcement of terms and conditions so long as certain pre-determined criteria within their coding is met (this study's definition of

[604] Article 30(2) of the draft Data Act.
[605] Article 30(4) of the draft Data Act.
[606] Article 30(5) of the draft Data Act
[607] Article 30(6) of the draft Data Act
[608] Josef Drexl et al, Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (2022) Max Planck Institute for Innovation & Competition Research Paper No. 22-05, 61.
[609] https://www.mydata.org/2022/10/25/amendments-to-the-eu-data-act/.
[610] https://www.bitkom.org/sites/main/files/2022-09/20220919_Data_Act_Standardisation_Tools.pdf.
[611] The importance of this distinction has also been stressed by E. Mik, 'Deconstructing Smart Contracts' (2022) Tilburg Law School Research Papers, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4239312.

smart contracts) would be an exercise of regulatory overreach that would considerably stifle innovation.

Beyond interoperability, model contractual terms have been identified as the second policy recommendation that could help facilitate the role of PIMS using smart contracts in the implementation of the draft Data Act's anticipated data portability regime.

Model Contractual Terms

Our analysis has unveiled that the complexity of EU data law as well as open questions emerging, inter alia, from uncertainties regarding the interaction between different legislative texts, in particular data protection law and the draft Data Act creates transaction costs for PIMS and partially subjects the operation of the latter to a lacking legal certainty. In order to remedy this, it has, for example, the German Ethics Commission has suggested to revise the GDPR in order to create a more specific legal framework for PIMS that enhances legal certainty.[612] The German Ethics Commission deemed that PIMS can only work efficiently where there is a legal obligation for data controllers to ensure that PIMS have access to personal data and to transfer any relevant information to the PIMS so that the latter can act in the interest of the data subject. For this a sector-specific solution was advocated.[613] At the same time, it should be ensured that data are not centrally stored to prevent cybersecurity risks.[614]

Our analysis has highlighted that model contractual terms could play a valuable role where personal data management tools are used in order to implement the draft Data Act's planned portability regime. They could reduce the transactions costs that arise in such contexts and enhance transparency as well as reduce legal certainty, particularly where smart legal contracts are used, they raise some tricky legal questions by their very nature. Our interviews with industry have indeed confirmed that model contract terms could facilitate data-sharing through PIMS.[615]

Model contractual terms could address open legal questions and, moreover, also provide legal solutions where there are no technical solutions to solve a given problem. To illustrate, we have also discussed an important technical limitation of PIMS, namely that once data is in the hands of a new data holder/data controller, it is no longer computationally possible to restrict usage of that data beyond the control of the original data user. Our industry interviews have suggested that this technical limitation could be addressed through legal means, such as in assigning usage rights and implementing access control and tools through an auditing process.[616] Model contractual terms could be useful in defining the modalities around this. Indeed, it was suggested that model contractual terms could resolve legal uncertainty and costs associated with implementing compliant solutions.[617]

In light of the above it is hence not surprising that there have already been industry initiatives on model contractual terms.[618] Academic research has led to similar conclusions as it has been stressed that one of the factors currently limiting the adoption of PIMS are

[612] Gutachten der Datenethikkommission (October 2019), p. 134.
[613] Ibid.
[614] Ibid.
[615] Interview with iGrant.io.
[616] Interview with O.Team.
[617] Interview with Datafund.
[618] Interview with iGrant.io. For an example, see further https://github.com/decentralised-dataexchange/data-exchange-agreements.

differences in their respective policies.[619] Indeed, this research highlighted that "privacy policies of organisations could vary according to their needs, goals, values, priorities and jurisdiction" which means that "the collection, use and retention of personal data would be done in different ways by different data consumers".[620]

Others have likewise suggested that model terms and conditions for PIMS should be the basis for certification and mandating companies to cooperate with certified PIMS in order to ensure high, trustworthy minimum standards for PIMS.[621] This research has suggested that elements on which the certification is based should include minimum standards for IT security, and restrictions on data access for affiliated services and transparency requirements.[622]

The German federal consumer protection organisation stressed the need for a new legislative framework for PIMS, which determines the boundaries within which PIMS can act, what kind of fiduciary duties they have, which ensures neutrality and acts against conflicts of interest and which provides for control and enforcement mechanisms and also ensure that these intermediaries do not have a self-interest in the further processing of personal data.[623] At the same time, they concede the narrow substantive leeway for any such legislation given how comprehensively the GDPR already regulates the processing of personal data.[624] The suggested solution was to introduce quality standards that enable data subjects to verify the quality of the PIMS, considering their limited ability to do so themselves.[625]

Model contractual terms could achieve the same objective. They could help address some general risks related to PIMS, such as that they could be used to manipulate the data subject to consent to sharing data against their actual will[626] or rely on dark patterns in order to reduce the data subject's informational self-determination.[627]

The analysis has identified that model contract terms could, for example, be helpful for the contracts required in the context of Articles 3-7 of the draft Data Act as well as to legally define certain common purposes of data sharing under the draft Data Act for common scenarios, respecting the fact that a purpose needs to be identified in relation to each processing of personal data and data protection law; to create specific requirements of transparency under both legal instruments and to govern smart contracts' compliance with consumer protection law, such as in respect of the requirement to draft contracts in natural language.

[619] Lachlan Urquhart, Neelima Sailaja, Derek McAuley, 'Realising the Right to Data Portability for the Domestic Internet of Things' (2018) 22 Personal and Ubiquitous Computing 317.
[620] Ibid, p. 25.
[621] Aline Blankertz and Louisa Specht, 'What Regulation For Data Trusts Should Look Like' Stiftung Neue Verantwortung (2021), p. 30.
[622] Ibid.
[623] Verbraucherzentrale Bundesverband, 'Anforderungen des vzbv an 'Personal Information Management Systems" (PIMS) und Datentreuhänder (2020), 4.
[624] Ibid.
[625] Verbraucherzentrale Bundesverband, 'Anforderungen des vzbv an 'Personal Information Management Systems" (PIMS) und Datentreuhänder (2020), 8.
[626] Ibid, 7.
[627] Gutachten der Datenethikkommission (October 2019), p. 133.

4. Concluding remarks

In this final section, the main takeaways from the economic analysis, the comparative law analysis, the technical feasibility assessment and the analysis on the personal data management tools are displayed.

The economic analysis has revealed that smart contract adoption in the EU at present is negligible in terms of economic value, thus no evidence of the use of smart contracts in cross-border transactions was found. The cost of current solutions is high, and the economic operation depends on a minimum efficient scale that is currently not achieved at the market level (profitable examples may exist at the enterprise level and in one-off projects).

Beyond that, the economic analysis found that the economic advantages of blockchain-based smart contracts are most likely to be present in high-volume markets (in terms of either a large number of market participants or a large number of transactions, or both). Such economic advantages include, among others, financial services, data management, as well as wholesale roaming.

Moreover, it was found that smart contracts related to B2B applications are more likely to see take-up as they face fewer constraints on contract formation. In addition to that, the deployment of smart contracts is easier in markets where transaction complexity is low and where transactions stay on chain, with no requirement for frequent conversion to outside currency.

The findings of the comparative law analysis allow the study to draw the following conclusions. First, the number of EEA Member States with smart contract legislation is low and the application of smart contracts in the internal market is negligible, as demonstrated by the economic analysis. Second, it has been shown that EEA Member States with specific legislation face no less challenges than those without such legislation. Third, no obstacles in the internal market could be identified due to the economically insignificant use of smart contracts at this moment in time, as has been revealed by our economic analysis.

The study has defined an obstacle as a diverging mandatory measure (typically a civil law rule) in an EEA Member State, which has the effect of preventing or hindering fundamental freedoms or distorting competition within the internal market.[628] An obstacle for smart contracts is a diverging mandatory measure (typically civil law rule) that actually prevents or hinders the uptake and roll-out of smart contracts within the internal market, while challenges are defined as potential obstacles and/or rules that are not easily compatible with the smart contracts technology. Given that there is currently no economically relevant uptake of smart contracts in the internal market, fragmentation of national laws cannot be qualified as an obstacle due to its relevance for the actual exercise of fundamental freedoms and competition in the EU. Yet, these measures are challenges – which have

[628] Case C-376/98 – Germany v Parliament and Council (*Tobacco advertisement judgment*).

been defined as potential obstacles – due to the fact that they would have such a practical effect if there were a broader uptake of smart contracts.

Fourth, the study has identified a number of challenges which, if smart contracts become used more widely in the future, could become obstacles to the use of this technology across the internal market.

The three main challenges stem from diverging EEA Member State measures (including contract law rules), also potential uneven technological conditions between EEA Member States (i.e. the level of existing technological infrastructure, as well as the investment in new technologies and their infrastructure might differ in EEA Member States) to apply and access smart contracts and other rules which are difficult for the smart contracts technology to comply with. The latter can include not only diverging but also harmonised rules which are difficult to comply with, such as, for instance, consumer law requirements in B2C contracts (e.g., right of withdrawal, information requirements etc). However, it should be borne in mind that these requirements, while a challenge from a legal perspective, do not necessarily qualify as such from the techno-economic perspective.

Civil law rules in EEA Member States could indeed pose challenges to the use of smart legal contracts, both at the national level and cross-border. These challenges are due to either the specific nature of smart contracts (e.g., immutability; program code as language) which seem incompatible with civil law rules and/or the attributes of contract law principles or provisions, which might be difficult to apply to smart contract technology and thus to ensure compliance (e.g., interpretation of intention, the requirement of the lawful and/or moral character of the contract). Potential discrepancies regarding smart contracts in EEA Member State legislations, as well as legal uncertainties around the application of the general rules on smart contract technology are also challenges.

Additionally, specific contract law rules in certain EEA Member States can create obstacles if smart contracts were used. In some cases, it is certain that the technology smart contracts are based on faces difficulties complying with rules in their present form, and the law should be adapted. This holds particularly true for specific form requirements for contracts as set out in national provisions (e.g., the requirement of notarial authentication or registration with public authorities). According to the data collected through this study, ensuring compliance of smart legal contracts with contract law rules poses challenges horizontally (e.g., identifying the contracting parties or interpreting tailored provisions) and in a wide range of sectors (e.g., property law, insurance law, loan contracts). In particular, challenges exist in consumer law (e.g., clear and legible terms, the consumer's right to withdraw from the contract).

The technical analysis has shown that many potentially promising use cases for DLT-based smart contracts exist in economically important markets (financial services, data management, communication) and in important emergent technologies (autonomous systems, PIMS). Cross-border transactions may be assumed to be particularly attractive use cases especially if transactions remain on chain, and the more so the lower the level of prevailing institutional trust transacting parties can rely on. However, this advantage is reduced if there remain substantially different national rules for smart contracts. Harmonised rules setting out, for instance, requirements for B2C contracts, can also be a challenge from a legal perspective, as noted above.

This study benefited from a comparative law analysis to determine commonly recurring challenges (see table 3) to the use of smart contracts in the EU/EEA. The case studies showed that there is a wide margin between the use of DLT in different business cases and for how smart contracts are eventually deployed. Many companies still opt for conventional written form contracts to underscore their legal obligations without doing this ‘on-chain.’ Identifying counterparties was viewed as a challenge while interpreting smart contracts in court proceedings and/or other forms of dispute resolution faces headwinds. Nonetheless blockchain-based dispute resolution could have a positive impact but is unlikely to displace national court proceedings in the near future. The examples in the study are small pilots or otherwise limited forms of Alternative Dispute Resolution making use of blockchain technology in the process.

Our study found that, in principle, requiring safe termination and interruption for smart contracts, archiving and auditability are not disqualifying features *per se* and depend also on the degree of openness of the ledger they are deployed on. In many cases, such as within the IoT sector, such features are welcome. However, they should be carefully calibrated with an understanding of their sectoral impact across both permissioned and permissionless blockchains. Without such assessment, there is a likelihood that such provisions if applied beyond the scope of the draft Data Act could stifle smart contract development and innovation in the EU. There exists a large body of rules and regulations that underpin the European legal order and it would be contrary to assume that smart contracts should be excluded in totality. However, the nature of the technology could make rules difficult to adapt or comply with. Using the draft Data Act as a unit of analysis, it was shown that this can be difficult even when rules are tailored to account for and include smart contracts. This has been found especially in the case of public-permissionless protocols. Reverse transaction features were discussed as an additional technical solution. It was found that they carry the potential for novel forms of on chain charge-back fraud when applied to public permissionless protocols.

The study found that standardisation initiatives are being developed both at EU level and globally to harmonise the specifications for smart contracts with ETSI and CEN CENELEC, driving draft Data Act supporting specifications for the EU and Blockstand, thus providing a pathway for international harmonisation. Embedded supervision could exist at both the hardware and software level when considering smart contracts applied to IoT. In the broader context, embedded supervision would have to be weighed in terms of balancing compliance needs with enabling innovation so as not to encourage a crowding out dynamic for smaller companies unable to shoulder the associated costs. Advancements in the field of digital identity could open new pathways for the machine economy and provide a vehicle to support both supervisory requirements and mitigate some of the smart contract risks identified in this report.

The final part of this study examined personal data management tools, which promise better control over data. PIMS are still a nascent group of technologies with different business models and which also use different technologies, sometimes including blockchains and smart legal contracts.

PIMS using smart contracts can facilitate the conclusion of a contract between the data holder and the data subject meaning that they can be helpful tools to enable access to data after a simple request through electronic means. We also find that PIMS can enable data users to easily verify their identity and facilitate data holders’ management of user information.

Smart legal contracts are particularly helpful under Articles 3-5 of the draft Data Act, as they can automate the conclusion and execution of such contracts subject to the limitations identified through the comparative law analysis in this study and hence reduce the costs associated with data-sharing.

PIMS using smart legal contracts must be careful to abide by the various legal requirements under the draft Data Act, the GDPR and national legislation and they must furthermore be designed so as to account for different interests, such as those of the consumer and the trader respectively where supranational consumer protection law is applicable, as well as the respective interests of the data subject and the data controller in data protection law.

Our research has identified two tools that could remedy some of these concerns: interoperability and model contractual terms. These two tools could, on the one hand, encourage the proliferation of compliant PIMS using smart legal contracts in the Digital Single Market and, on the other, make it more attractive for relevant actors to rely on PIMS using smart contracts.

Annexes

Annex I: Questionnaire template for national legal research

In answering the questions below, please take into account the following:

- ***Please answer these questions succinctly but completely, always referring to the relevant sources and legal provisions (and adding a link).***
- ***While the answers should generally cover the national/federal level, please include anything of note at the regional/state level.***
- ***Please answer all questions based on legislation specifically applicable in relation to a certain topic, or in absence of this, on the general legal regime that applies.***
- ***Where available, please provide information on case law in your country, if there is any, per section/general issue (i.e. contract formation, form requirements etc).***
- ***Please indicate in your answers whether the rules mentioned are expressly mandatory or have a mandatory effect in your legal system.***

Introductory questions

1) **Is there any legislation in place relating to the use of distributed ledger technologies and/or specifically applicable to smart contracts in the scope of this study in your country? If so, please provide an overview of the applicable legislation. Has this applicable legislation had an effect (whether incentivising or negative) on the adoption of smart contracts in your country?**

2) **Is a definition of smart contracts set out in the national legislation? Are there any specific rules regarding the types of smart contracts – e.g. code-only, ancillary smart contracts or Ricardian contracts – allowed in your country?**

3) **Are there any specific sectors in which the use of smart contracts is regulated or where particular challenges (e.g. as regards form, language etc.) for smart contracts exist? If so, please elaborate.**

Contract formation

4) **Where and when is a contract considered to have been formed/created/concluded, according to your national laws? Do any of the constitutive elements of a contract – offer, acceptance, intent – require any formalities other than the parties' consent? Especially as regards the**

declaration of intents of the parties, when are they deemed to have been exchanged? Does any of these formalities constitute a challenge for a smart contract to be considered formed/created/concluded, in your legal system?

5) **What legal requirements need to be met under the applicable law in your country for a contract to be valid, binding and enforceable? This includes relevant legal requirements on existence of a valid, binding and enforceable contract (e.g., certainty/clarity of terms; differences between B2B and B2C contracts). Does any of these requirements constitute a challenge for a smart contract to be considered valid, binding and enforceable by law?**

6) **Are there any explicit requirements regarding the identification or the number of parties in a (smart) contract? If yes, what problems may this pose as regards smart contracts?**

7) **Is an obligatory verification of the reliability of the code by an auditor or trusted third party (TTP) foreseen in the national legislation?**

8) **Are there any specific requirements in your country regarding the choice of applicable law in cross-border transactions, which may discourage the choice of smart contracts as means for such a transaction? Is there any case law available in your country on the above issues, as regards smart contracts?**

Form requirements

9) **Are there any general or sector-specific (e.g. transfer of immovable property, shipping/transport documentation) form requirements for agreements in your country (e.g., conditions that must be met for an agreement to be deemed valid)? If so, can such form requirements constitute limitations to the use of smart contracts as transactional means?**.

10) **Are there any legal requirements regarding the form of "passive" contractual terms (e.g., clauses on liability, choice of law/jurisdiction, statutory clauses) in your country? If so, do they pose a challenge for smart contracts?**

11) **Are there any specific requirements (e.g., conditions that must be met and which), for electronic contracts to be considered valid in your country (e.g. as regards signatures)? Can they apply to smart contracts?**

12) Are there any provisions equating smart contracts (in terms of legal validity) with prose contracts with written or electronic signatures?

13) Are there any specific requirements regarding 'durable mediums' in your country?

Contract interpretation/evidential value

14) Are there any rules for the interpretation of agreements in your legal system? What would be the main challenges posed by them, in relation to the interpretation of smart contracts (e.g., terms which incorporate elements of subjectivity on behalf of the parties, or terms the nature of which is not specific)?

15) Are there any specific requirements in your legal system for agreements to bear full evidential value in the context of (court) claims? What would be the main challenges posed by them, as regards smart contracts?

Civil and Consumer law requirements

16) Can you identify any situations in your country where specific legal requirements (and which) would not allow for the deployment and lawful performance of a 'code-only' smart contract from a civil and consumer law perspective?

17) How does the legal system in your country treat agreements that contain unfair terms/conditions or terms/conditions that have been expressly declared invalid by court? Can such treatment pose a challenge to smart contracts?

18) Do consumer law requirements apply to smart contracts (i.e., do smart contracts fall within the scope of consumer protection laws) in your country? Overall, what effects do the consumer protection law requirements may have on smart contracts?

19) What specific information are the traders required to provide in a contract and in what form/language according to national rules transposing Articles 6 and 8 of the Consumer Rights Directive and Article 10 of the E-Commerce

Directive? Can these or other national rules, which set out additional information requirements, present a challenge to smart contracts?

Termination of contracts and remedies

20) Are there any specific provisions on the right of withdrawal or the right of suspension (e.g., in case of force majeure) which can pose a challenge for smart contracts?

21) Which remedies are available/applicable to (smart) contracts under the applicable law, in case a smart contract is void or declared so by court?

22) If any remedy requirements are foreseen, do they present a challenge for smart contracts? If yes, what are those challenges? Are these remedy requirements mandatory or effectively mandatory (as per the Tobacco advertising judgment)?

23) In what cases do the national restitution rules (if any) apply to smart contracts?

24) In case a contract is terminated, including based on consumer law remedies, how do the applicable rules apply to smart contracts?

Concluding remarks

25) What is/are, in your opinion (please justify), the cause/s of legal uncertainty, if any, as regards the use and deployment of smart contracts in your country (e.g., lack of legal frameworks, lack of standards, etc)? Is there any case law or are there any publications/discussions in the national academic literature on this subject?

Annex II: Scale of the impact of smart contracts based on DLT

It is difficult to obtain an empirical picture of the state of smart contract adoption in Europe. To describe the real state of adoption of smart contracts, it is not enough to look at the simple metrics such as the number of existing smart contracts in a blockchain network (there might not be a real use case or interaction with real users, there is large variation in how often contracts are executed, etc.).

Moreover, a breakdown that shows smart contract adoption in the European Union is not feasible with the data that was reviewed as part of the project[629]. The key reason is that blockchain platforms are not limited to specific geographic regions, rather they are available to all users globally. Moreover, the technology is still developing rapidly and in different directions, which makes a comprehensive picture at any point in time inherently difficult to obtain. This section takes a pragmatic approach to synthesise a number of high-level data sources to paint a broad-brush picture of the state of global smart contract adoption.

Verified contracts

One approach to understanding the growth of smart contracts is to analyse the daily growth of verified smart contracts, such as those provided by trusted block explorers. Once a smart contract is verified the smart contract's source code becomes publicly available. 2022 data[630] shows values of approximately 1,000 to 2,000 daily smart contracts on the Binance Smart Chain, and values in the low hundreds for Polygon and Ethereum as the three largest chains by this metric. The verified data about smart contracts should not be confused with the total number of smart contracts deployed on the blockchains. This number is not sufficient to describe the current state of adoption on a particular blockchain but provides an indication of the engagement with smart contracts.

Approximation based on the number of replaceable contracts

While the data provides some evidence on significant activity levels around DLT smart contracts, there is no robust empirical data on smart contract adoption in relation to economic activity.

A first order approximation of the benefits of smart contracts can be made by considering the number of current, non-smart contracts between human parties that can be replaced[631].

A crucial characteristic of smart contracts, as opposed to traditional contracts, is that the former only exist to be executed (if the conditions that trigger the encoded actions are met), and in fact their value increases with the number of executions; while the latter fulfil at least some of their functions (e.g. protecting against risk) even if – or especially – if they are never enforced/executed.

[629] The lack of such data was confirmed both through desk research by the team and expert interviews.

[630] See EUBOF Smart Contracts report (2022). Compares new verified smart contracts across the Ethereum, Polygon, REUM, Binance Smart Chain, Avalanche, and Optimism Blockchains. These networks were selected because the methodology used by their respective block explorers to extract the data is the same, while other blockchain explorers use different methodologies.

[631] The 'smart contracts' used in machine-to-machine transactions and pure process automation applications (i.e. using an algorithm to trigger actions instead of deliberate action by a human operator) are not included in the definition.

The benefit of smart contracts come from improved performance at the point of execution: the speed, ease and reliability of performance, which is also scalable.

The benefit of smart contracts is then the reduction in the need for traditional contracts, a reduction in conflict over the performance of a contract, leading to reduced litigation.

How large could this impact be? The starting point is that the number of traditional contracts is very large, and the number of times contracts are performed is much larger still.

Table 10: Contract performance by individuals (illustrative example)

EU population	447,000,000
Average number of contract executions per day (assumed)	20
Total number of contract executions (per year)	3,263,100,000,000
Average number of contract executions per person per year	7,300

Table 11: Contract performance by enterprises (illustrative example)

Turnover band	Number of enterprises	Average number of contract executions per enterprise per year (assumed)	Total number of contract executions
Less than €1 million	21.7 million	7,300*	158,410,000,000
€1 million to €10 million	2.1 million	50,000	105,000,000,000
€10 million to €50 million	0.2 million	100,000	20,000,000,000
€50 million to €250 million	0.03 million	200,000	6,000,000,000
€250 million to €1 billion	0.004 million	1,000,000	4,000,000,000
Greater than €1 billion	0.0008 million	10,000,000	8,000,000,000
Total (per year)			301,410,000,000

**** assumed to be = contract performance by individuals. ** Source: Eurostat, Structural Business Statistics (2019).***

Taken together, there may easily be over 3 trillion instances of contracts being performed in the EU per year.

Not all these can or will be implemented as smart contracts. Paper contracts retain some comparative advantages, not least that the performance cost of a paper contract is zero, whereas every execution of a smart contract has a cost, so that the marginal cost of implementing another smart contract will exceed the benefit. At the same time, the number of paper contracts that can be replaced is likely to be large, especially as there are many cases where multiple contracts can be simplified into one smart contract.

In summary, the scale of the potential benefit from replacing paper contracts with smart contracts in the EU is very large. The economic value of the technology and consequently the value of removing civil law obstacles is no doubt positive over the medium term. The size of the benefit, however, is very uncertain.

Benefits at the use case level: deltaDAO, CashOnLedger, Bosch examples

Given the lack of robust data on the costs and benefits of smart contracts and the uncertainty over potential future use cases and scale of deployment, little can be said about the overall value of smart contracts for the European economy beyond the high-level assessment provided above.

However, to characterise the potential value of removing obstacles found in Member States' civil law it is useful to distinguish the source of benefits at the infrastructure level that drives benefits at the level of individual use cases. In the 3 use cases reviewed in detail in this study (detaDAO, CashOnLedger, Bosch), 3 sources appear prevalent, and the overall benefit is typically a mix of all of them.

- **Automation**: by replacing increasingly complex processes and interactions between different (human and machine) entities with smart contracts, benefit of automation can be achieved in many settings.
- **Enabling new applications**: this is a necessarily broad category of benefit that reflects the platform/ecosystem nature of smart contracts, which offer scope for new solutions using the technology to be created.
- **Replacing non-smart contracts** with a mechanism that has significantly lower 'per-execution' cost and potentially lower setup cost.

While the first two clash with existing legal frameworks to some extent (this is discussed in greater detail in the technical feasibility assessment), it is the last point where there is the clearest role for civil law to ensure that inefficient current forms of contracting[632] are replaced where possible with 'smarter' contracts.

Table 12: Overview of benefits at the use case level

Example	Automation	New applications	Potential to replace traditional contracts
deltaDAO	Can streamline analytics workflows involving sensitive data.	Enables certain types of analytics without sharing data. Potential for new service offerings in third party analytics.	Potentially large-scale replacement of contracts as the infrastructure obviates certain compliance and risk issues (GDPR, cybersecurity). Especially benefits small companies, who may face uninsurable data security risks, or -

[632] See e.g. Hoffman, D. A. (January 22, 2023). Defeating the empire of forms. University of Pennsylvania, Institute for Law & Economics Research Paper No. 23-04. http://dx.doi.org/10.2139/ssrn.4334425 for a summary of the pervasive problems with traditional form contracts.

			for lack of a track record - cannot generate sufficient trust to obtain data However, there are still non-smart terms and conditions attached to using the infrastructure.
CashOnLedger	Can streamline asset leasing and rental processes	Potentially very widespread applications in IoT, with applications for both industrial assets and consumer products.	Could obviate a number of contractual relationships, e.g. around long term leasing of assets (smart home and transportation in the consumer market), all sorts of industrial machinery. On-chain payments could reduce the need for payment-related contract infrastructure.
Bosch	Car-to-car communication to enable smart transportation systems. Potential for software agents that act on behalf of their owners for economic benefit.	Potentially very widespread applications in smart mobility.	Potential for the replacement of traditional contracts in areas like insurance (automated claims and settlements) and service contracts (e.g. access to toll roads, parking space). On-chain payments could reduce the need for payment-related contract infrastructure.

In line with the discussion above, a lot of the value will be realised at the level of individual applications (from automation of existing applications and entirely new applications), which are currently immature. However, at the system level, the replacement of traditional contracts with smart contracts creates a distinct economy-wide benefit. The size of this benefit depends on the current per-execution cost, the cost of using the smart-contract infrastructure and the cost of avoided litigation in a given setting, which is again likely to be highly variable across applications.

Annex III: Feasibility Matrix

The Feasibility Matrix reflecting the three case studies can be found in a separate file (Excel format) annexed to this final report.

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
– at the following standard number: +32 22999696,
– via the following form: european-union.europa.eu/contact-eu/write-us_en.

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

EU open data

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

<Catalogue number>

Publications Office
of the European Union