European Crypto Initiative

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

THE DATA ACT SMART CONTRACTS
IMPLICATIONS FOR THE FUTURE OF INNOVATION IN EUROPE

INTRODUCTION

Europe is at a crucial point in setting down rules governing the use of innovative technologies such as AI, Blockchain and quantum computing, especially as it strives to bridge the gap with other jurisdictions that have more fully grasped the countless benefits of Web1 and Web2 innovation.

Significant progress has been and continues to be made to strengthen the Digital Single Market during this mandate (through the Digital Markets Act, Digital Services Act, Artificial Intelligence Act, European Digital Identity framework, and Data Governance Act), providing Europe with a strong basis for the establishment of a coherent legal framework for data sharing through the Data Act.

This final significant piece of Europe's digital strategy can enable a European vision for a free, open, and secure global internet where citizens have control over their data; it holds the promise of a dynamic data ecosystem that can harness and unleash a new data-driven economy that strengthens the competitiveness Europe while safeguarding its most important principles and values.

To unleash the full potential of Europe's vibrant, innovative data ecosystem, Europe needs clear, fair, and forward-looking regulation, which can serve as a stepping stone towards enabling innovation. A key part of achieving this goal is fostering seamless data transmission with full transparency, autonomy, reduced cost, and speed. Automatised and digitally executed contracts (i.e. the "smart contracts") play an increasingly essential role in this respect, and the technology that underpins smart contracts is constantly evolving. Europe will be among the first jurisdictions to regulate the use of smart contracts through the Data Act. It is essential to get it right.

In the context of the ongoing trialogue negotiations on the Data Act, we, together with the 18 organisations listed at the end of this paper, wish to share a number of concerns that we have regarding the treatment of smart contracts so that Europe doesn't "shoot itself in the foot" by inadvertently damaging innovation and technological development in the broader Blockchain industry - given that much of that innovation is happening in the Web3 enabling technology that relies on smart contracts that do not fit the current provisions of the Data Act but would likely be captured.

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

1. TECHNICAL AND LEGAL CLARIFICATIONS

1.1. Definition of Smart Contracts

While ‘smart contracts’ generate attention for their potential uses, no explicit consensus exists around the term. Some refer to it as *digitally composed and executable agreements*, and others use the term as a niche that refers to a *specific set of code* that utilises distributed ledger technologies (DLT) to execute orders.[1] There is widespread recognition, yet different meanings are assigned to the term ‘smart contract’ by the blockchain industry, as well as regulators across the globe. To this day, the DLT is widely regarded as the most optimal technology to drive the next-generation Web3. We are concerned that the current scope and wording of the Data Act may inadvertently encompass smart contracts based on DLT, which by their inherent nature and design, may prove difficult or even impossible to comply with certain requirements proposed in the Data Act and may hinder the development of this novel technology, which the Union seeks to support. This is particularly relevant for smart contracts based on decentralised DLT infrastructures, which constitute the overwhelming majority of smart contracts deployed and used now. For these reasons, we ask the co-legislators to clarify that the Data Act does not cover DLT-based smart contracts in the domain of IoT data sharing.

a) **It is our observation that the discrepancies described above may be resolved by using different terminology. Thus we respectfully suggest that the co-legislator adopts a different term and uses ‘digital contracts’ instead of ‘smart contracts’ as the latter has already gained recognition and adoption within a broader Web3 industry.**
b) **Would the regulator refuse the change proposed above, we respectfully suggest that co-legislators provide necessary clarifications with respect to Article 2 (16) in the Council position, which contains the definition of 'smart contract', by clearly differentiating between a digitally executed legal agreement (digital contract) and a computer code, commonly referred to as a 'smart contract utilising distributed ledger technology (DLT)' and excluding the latter.**

[1] See existing ‘smart contract’ definitions adopted by Japan Payment Service Act (JPSA); United States Law Commission's Uniform Electronic Transactions Act proposal (the LG Act); the UK Law Commission’s Smart contract call for evidence and UK Jurisdiction Taskforce (“UKJT”) legal statement on cryptoassets and smart contracts; ISO 22739:2020; and COALA's DAO Model Law.

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

It is pertinent to note that the consideration and acceptance of either point a) or b) above may be sufficient for achieving the aim of this Position Paper. Therefore, the acceptance of either point above renders the remainder of this Position Paper unnecessary to implement in practice.

c) **In the event that neither of the aforementioned points, a) or b), finds acceptance by the co-legislators, it is respectfully submitted that a more confined interpretation of a term 'smart contract' would be preferable to prevent the application of the Data Act without due consideration of relevant technical distinctive features. To this end, we suggest a more limited definition of a 'smart contract,' one that is exclusively applicable to legal contracts and technical tools or implementations thereto that permit automatic data sharing among IoT devices. Such a tailored approach would ensure a more precise and focused regulatory framework while also accommodating the technical intricacies of smart contracts in an appropriate and effective manner.**

1.2. Scope of Article 30

The Commission proposal primarily targets data that is "*generated by the use of a product or related service available through or related service available to the user of that product or service, on the making data available by data holders to data recipients, and on the making data available by data holders to public sector bodies or Union institutions, agencies or bodies, where there is an exceptional need, for the performance of a task carried out in the public interest*."[2] While the Data Act focuses on IOT products, the wording of Article 30 leaves room for a much wider interpretation and might unintentionally capture a much broader blockchain industry and consequently give rise to significant and unintended economic consequences.

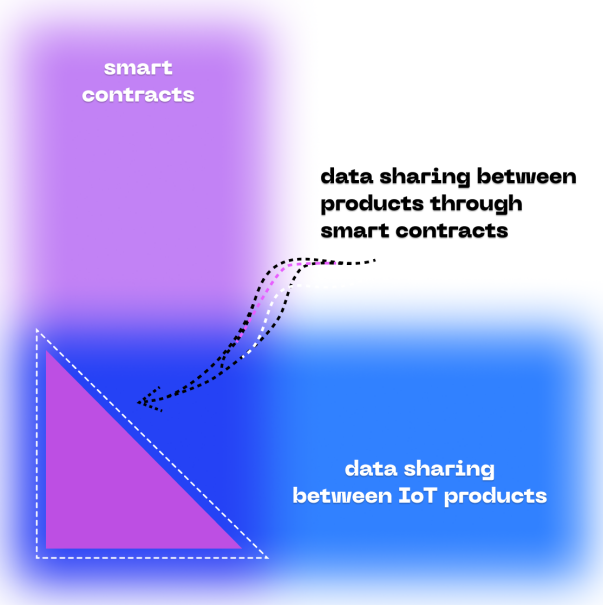
As such, Article 30 should be clearly aligned with the intention of the Regulation, which is on the use of smart contracts in the context of IoT devices and data sharing between data spaces.

We recommend that co-legislators clarify the scope of Article 30, delineating the specific types of smart contracts that fall within its purview, and stipulate that Article 30 does not apply to

[2] Article 1 (1) of the European Commission draft. If not stated otherwise, all the cited articles come from the Commission's proposal for Data Act.

DLT-based smart contracts. This would serve to better align the provisions of the Data Act with the original goal of the proposal and ensure legal clarity as well as consistency.

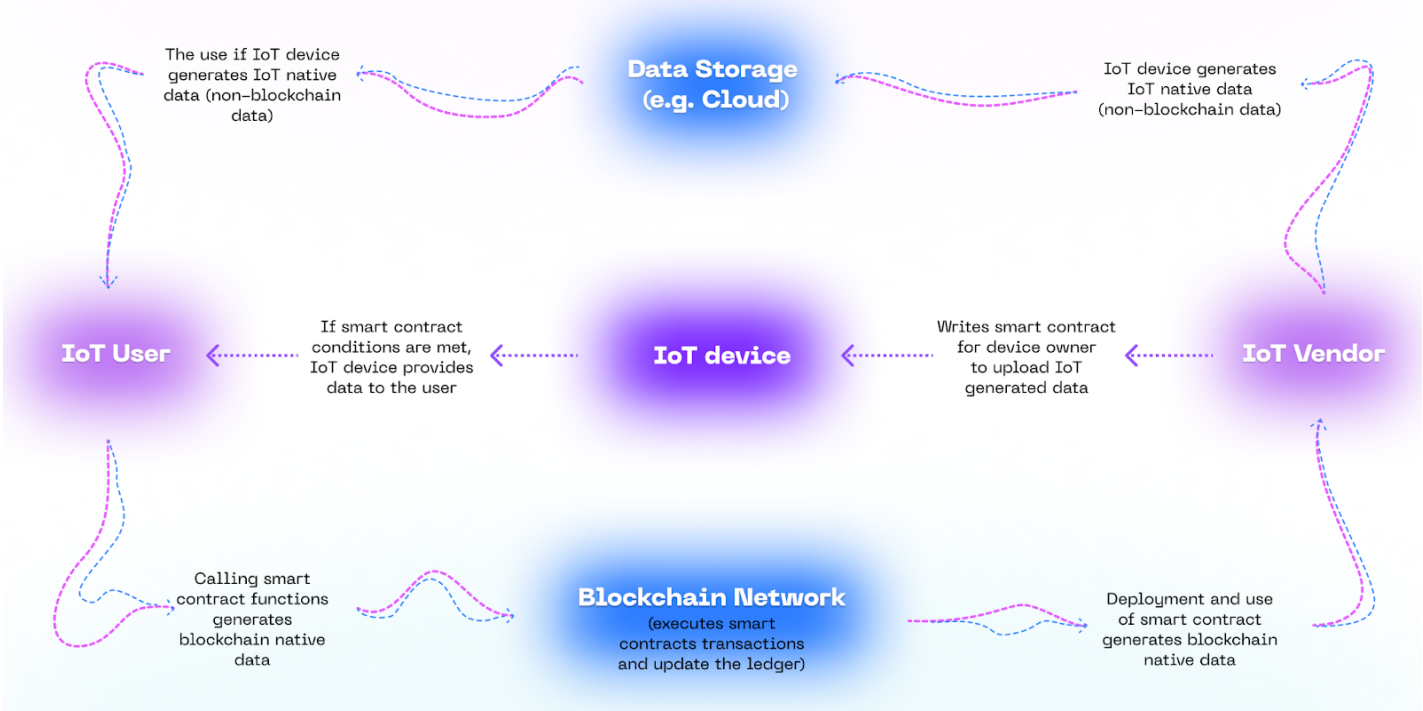
The potential economic ramifications of the uncertainty surrounding current permissible use cases of smart contracts for data sharing cannot be overstated. Any ambiguity in this regard may disproportionately hinder the use and development of smart contracts or even de facto prohibit them. Compliance would be practically impossible for those smart contracts vendors that rely on public blockchain technology, as such smart contracts typically transmit data openly through records that are accessible on the blockchain. Our current assessment suggests that the vast majority of smart contracts in use are developed on public blockchain technology. Thus, a definitive understanding of the compliant use cases for smart contracts, particularly those based on public blockchain technology, must be established to avoid any potential adverse outcomes. Below, we're attaching a graphical representation of the intersection between all possible applications of 'Smart contracts' and 'Data sharing through IoT devices'. We argue that the scope of Article 30 should be limited to that intersection.



1.3. Clarification of Data Sharing

Clarification of "data sharing" is all the more needed because Article 2 (1) in the Commission proposal defines "**data**" as "**any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording.**" It should be noted that smart contracts can be made in such a way that a function triggers a transfer of any such data

from one digital wallet address to another.[3] As every single use of a smart contract generates data being shared publicly, the current text poses a risk of it being applied excessively broadly, that is, to those smart contracts that generate and publicly share data that is not generated through the use of IoT devices.
Whereas smart contracts may be used to share data produced by IoT devices, they are often used without any reference to an IoT device whatsoever (e.g. merely to confirm a certain transaction status between private parties). The distinction between the IoT and non-IoT data is, therefore, crucial to clearly indicate the regulator's intention to regulate smart contracts allowing for sharing the IoT data alone.



As the picture above shows, the mere use of a smart contract creates data that is not necessarily related to the data coming from the IoT device (non-IoT data).

We respectfully recommend that co-legislators ask for a thorough examination of the diverse categories of smart contracts that currently exist and, in the meantime, adjust the definition of "smart contract" contained in Article 2(16) of the Council Data Act position. This measure would enable a more targeted and streamlined approach to the application of the provisions of the Data

[3] Smart contract functionalities are called and triggered when a user requires certain actions to be performed. However, the information shared and transferred among various parties is often stored, generated, and transmitted locally (e.g. hosted and stored by the users themselves).

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

Act, precluding their broad and indiscriminate application to all DLT-based smart contracts, and instead, confining their scope solely to the specific use cases envisaged by the Data Act - that is, scenarios where smart contracts are employed for data sharing between products and data spaces.

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

2. SMART CONTRACT DESIGN FEATURES AND REQUIREMENTS

Article 30 of the Data Act includes a number of essential design requirements, such as robustness, safe termination and interruption, data archiving and continuity, and access control. We believe that the current wording may have potentially negative consequences for the DLT and blockchain industry as it will not allow for industries and developers relying on the DLT-based smart contracts to comply with the requirements.
Below we set out our main concerns regarding the compatibility of certain requirements with the unique design features of smart contracts (further information is provided in the Annex).

2.1. Responsible persons

Article 30 proposes that the responsibility for complying with smart contract requirements might fall upon developers of smart contracts who deploy smart contracts.[4] Vendors and/or persons responsible for the deployment of the technical 'smart contracts' utilising DLT does not have the means to comply with smart contract requirements as proposed in Article 30 of the Data Act. Further, when this is carried out in an open-source manner, for example, on behalf of or in the name of a vendor or the offerors, we deem the responsibility disproportionate and unjust. Such expansion of responsibilities from vendors to whoever deploys a smart contract should not be conditional upon the absence of a vendor alone; the regulation should further clarify the circumstances under which the responsibility transfers from a vendor to other persons. The Data Act should also strive to encourage the community to further innovate in this field and not obstruct or overly burden those who build valuable solutions, especially if such solutions are built for and on behalf of others (e.g. vendors).

Furthermore, while we welcome the Council's efforts to improve the text and ensure greater legal certainty,, the Council's latest text in **Article 1 (2) (f)** scopes in "*operators within data spaces and vendors of applications using smart contracts and persons whose trade, business or profession involves the deployment of smart contracts for others in the context of agreements to make data available*". We consider that this addition to the Data Act's general scope does not serve a clear purpose, as it doesn't refer exclusively to Article 30.

We, therefore, do not support the current wording of Article 1 (2) (f) in the Council position and ask that it is made clear that it only applies to Article 30.

[4] In the Commission's proposal and Council's General Approach on Article 30, the responsibility for complying with smart contract requirements is vested with the vendors or, in the absence of a vendor with a person "whose trade, business or profession involves the deployment of smart contracts for others in the context of an agreement to make data available". In the Parliament's position, responsibility is vested with the "offering party".

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

2.2. Immutability of Smart Contracts

The **immutability** of smart contracts (i.e. the inability to change their design or functionality) should not be considered a design flaw but a design feature. The reason is that, if removed, the smart contract will also lose the element of trust and security, which is of fundamental importance to its successful use.

2.3. Safe Termination and Interruption

Compliance with the provisions referring to the 'safe termination and interruption' could considerably increase the cybersecurity risks associated with the use of smart contracts as this could give rise to a single point of failure. DLT-based smart contracts are specifically designed to eliminate the possibility of safe termination as a measure to ensure the security of the code and prevent any potential data misuse or abuse. Compliance with provisions of Article 30 would necessitate a single point of failure for the safe termination and interruption of smart contracts, which increases the risk of potential vulnerabilities being exploited.

Due to the cybersecurity concerns described above, the termination or interruption functions are not optimum solutions to be implemented within the smart contract, as data, funds, and operations linked to the smart contract can be easily exposed.

Furthermore, smart contracts have gained recognition for being immutable and thus resistant to improper governance decisions or changes. Features like "hard termination"[5] could introduce some of the most significant risk factors in terms of security (e.g. single point of failure) and could have a great impact on the governance of the underlying protocols. Therefore, the burden of those responsible for complying with Article 30 would be accompanied by a greater security risk, which we deem unproportionate to the desired scope of the regulation, that is, IoT products.

In view of the above, it is paramount that the legal implications of implementing these requirements are carefully examined before they are included in the legislation to ensure that it does not compromise the integrity and effectiveness of smart contracts or the Data Act's objectives.

To ensure the efficacy of this Regulation, Article 30 must be tailored to apply exclusively to defined use cases of smart contracts for data sharing, where only a specified range of safe termination or

[5] See the Annex for more details about the difference between a "soft" and a "hard" termination of a smart contract.

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

interruption functions are enabled or designated to the parties responsible for utilising, implementing, and deploying the smart contract.

In addition, it is imperative for Article 30 to further stipulate requirements regarding smart contract access control. That is, Article 30 should establish who the persons responsible for resolving the errors or calling the termination function (and under which circumstances) are.

2.4. Interoperability and Standardisation

Moreover, while we encourage **interoperability and standard creation**, as well as integrating **access control**, we believe that they should be developed by the industry or standardisation bodies. Moreover, they should consider the technology's current development, especially considering that interoperability isn't tied to the developer's or user's preference but is rather limited to the DLT infrastructure of the smart contracts, which presents a technological specificity rather than a flaw.

Another potential issue that we recognise is that the establishment of standards at such an early stage of the technology's development might lead to narrowing the development of smart contracts to a specific subset.

Therefore, we do not support the Commission and the Council's approach towards standards development; standardisation requirements should only be introduced when the need for such standards has been duly considered and become apparent.

2.5. Equivalence requirement

We are concerned by the European Parliament's addition made to the Commission proposal, which calls for equivalence between "smart contracts" and what seems to be described as "legal contracts", as it is not feasible from a technical point of view.

As mentioned above, "DLT-based smart contracts" aren't contracts in nature but rather lines of code. Typically, they facilitate and automate the execution part of a contract or agreement. As such, we consider that there cannot be equivalence or the same level of legal certainty or protection provided solely within the code that the smart contract represents because of its inability to write complex text in human-readable language.

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

Therefore, we suggest deleting the proposal contained in the Parliament position in Article 30 (1) (ba).

2.6. Protection of Trade Secrets

Based on the definition of a trade secret,[6] our concern is that if the public data inherent to the use of a smart contract is part of the trade secret, the use of public blockchains, in this case, would be considered non-compliant.[7] Therefore, the current drafting creates some uncertainty that could cause confusion among both the responsible persons and entities under the Data Act and the competent authorities monitoring the implementation of these requirements.

We, therefore, do not support the inclusion in Article 30 (1) (bb) of the Parliament's position.

[6] According to Directive (EU) 2016/243, "'trade secret' means information which meets all of the following requirements: (a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) it has commercial value because it is secret; (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret". Therefore, it can be metadata, through which you can see that a party transacted a specific number of times per day and at a specific hour, information might be considered a trade secret if for example, it is used by a competitor.
[7] See also Graph 2 above.

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

3. CONCLUSION

For the reasons described above, we respectfully suggest the European legislator carefully examine the distinction and avoid interchangeable and potentially erroneous use of 'smart contract' terminology. Our understanding is that the Data Act is not intended to regulate the use of smart contracts in the broader blockchain ecosystem beyond the use cases envisioned by the Data Act (IoT and data sharing between data spaces).

We suggest that co-legislators clarify this point, and avoid interchangeable and potentially erroneous use of 'smart contract' terminology.

The absence of such clarification would have detrimental implications, including

- Lack of legal certainty would discourage the development of cutting-edge innovation;
- Lack of proper standardisation, instructions, and limitations would give rise to new cyber threats;
- Liability to comply with the above-mentioned requirements would hinder innovation (both from a cost perspective and funding opportunities).

Alternatively, we respectfully suggest that provisions of the Data Act be subject to the exclusion of 'smart contracts which utilise DLT technology'.

The European Crypto Initiative is a Brussels-based trade organisation that supports innovative & innovation-friendly regulation adapted to decentralised applications that leverage blockchain technologies. We believe it would be beneficial to continue this conversation, provide you with further details and comments and hear your opinion and concerns. Please feel free to contact us so we can set a meeting at your convenience: info@crypto-initiative.eu.

European Crypto Initiative

EU Crypto Initiative
Rd-pt Robert Schuman
1040 Brussels
Belgium

This position paper is supported by:

ADAN

BLOCKCHAIN FOR EUROPE

Blockchain Hungary Association

BLOCKCHAIN THINK TANK SLOVENIA

BB

BLOCKCHAIN LAWYERS GROUP

Canadian Web3 Council

CONSENSYS

DeFi Education Fund

DIGITAL CURRENCIES Governance Group

EUROPEAN BLOCKCHAIN ASSOCIATION

instituto new.economy

IOTA

LEDGER

MAMA Multichain Asset Managers Association

NORDIC BLOCKCHAIN ASSOCIATION

SPANISH CRYPTO ASSET ASSOCIATION

swarm

UBIK