Digital Society (2023) 2:9
https://doi.org/10.1007/s44206-023-00038-2

BRIEF COMMUNICATION

How to Improve Smart Contracts in the European Union Data Act

Federico Casolari[2] · Mariarosaria Taddeo[1,3] · Aina Turillazzi[2] · Luciano Floridi[1,2]

Received: 17 February 2023 / Accepted: 28 February 2023/ Published online: 18 March 2023

Abstract
The article analyses the role of smart contracts in the architecture of the European Union's Data Act proposal. It identifies five difficulties: lack of flexibility in terms of both content and operation; dependence on oracles which could lead to errors; vulnerability to bugs and changes in architecture; immutability and privacy; and problems of enforcement. It then offers some recommendations about how to address them to improve the Data Act.

Keywords Smart contracts · Data Governance · Data Act; Web3

The Proposal for the Data Act (the Proposal)[1] is an essential component of the European strategy for data (European Commission, 2020). It specifies who can create value from data (including data generated by the Internet of Things) under which conditions. It complements the Data Governance Regulation (November 2020), as a future regulation that is expected to harmonise and facilitate fair access to data and their use in the EU. These two new instruments need to be coherent with the General Data Protection Regulation ('GDPR') and complementary to it, given their shared goal of maximising data sharing (Czarnocki, 2022). The European Commission (the Commission) published the Proposal on 23 February 2022. As the legislative process is still ongoing, it may be useful to seek to rectify some potential shortcomings. In this article, we focus on how to improve the measures suggested in the Proposal for smart contracts.

[1] European Commission, 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.

✉ Luciano Floridi
luciano.floridi@oii.ox.ac.uk

[1] Oxford Internet Institute, University of Oxford, 1 St Giles', Oxford OX1 3JS, UK

[2] Department of Legal Studies, University of Bologna, Via Zamboni 27/29, 40126 Bologna, Italy

[3] The Alan Turing Institute, British Library, 96 Euston Rd, London NW1 2DB, UK

In the Proposal, the Commission gives smart contracts a key role in achieving its envisaged data governance architecture. The goal is to maximise the value of data by ensuring that a broader range of stakeholders gains control over their data and that more data is available for innovative use (European Commission, 2022). The underlying feature of the Proposal is to provide the Member States with a scheme for data sharing. Thus, data transfers and interoperability are central to this goal. They underpin the majority of the most important provisions of the Proposal, from the right of users to require their data to be shared, at no cost to them, by the data holder with a third party (Article 5) to the obligation to make data available to public sector bodies or EU institutions in cases of exceptional need (Articles 14, 15). The Commission sees smart contracts as a potential solution to make data transfers easier, and the Proposal lays down a regulatory framework for smart contracts and a new vision for how they should operate, at least in the context of data transfers.

The Proposal defines smart contracts (Article 2(16)) as being based on an 'electronic ledger system' where the outcome of their execution is also stored. It then suggests that they could be an appropriate technical measure to ensure compliance with its provisions (Article 11; see also Articles 5 on the obligation of data holder to share data with a third party at the request of the user; 6 on the duties on the third-party receiving data at the request of the user; 9, on the compensation for making data available; and 10, on dispute settlement). The Proposal sets out four requirements for smart contracts to make data available (Article 30): robustness, safe termination and interruption, data archiving and continuity, and access control.

Despite the broad support, and the steps taken in the Proposal to make smart contracts fit for purpose, the choice is problematic for many reasons (Ante, 2020), five of which are significant and should be addressed.

First, smart contracts are fixed in terms of content and operation. The difficulties of transposing natural language into code make the inclusion of specific clauses virtually impossible (De Filippi et al., 2021). At the same time, smart contracts are, by their very nature, 'tamper-proof'. This makes them unamendable, in line with the trustless nature of blockchain-based technologies. These two limitations are inherent to the foundation on which smart contracts are built, making it impossible to terminate them once executed. Thus, one of the essential requirements suggested by the Proposal, safe termination and interruption, seems to be at odds with the current functioning of smart contracts. However, one could achieve safe termination and interruption in two ways. Both require a move away from the use of smart contracts. On the one hand, one could rely on classic contract solutions. For example, a traditional contract could be adopted to regulate the relationship between the parties to the smart contract. The problem with this approach is that it defeats the very purpose of smart contracts. Or one could include traditional contract law remedies into the code underlying the contract. However, this is difficult because of the problems associated with transposing natural language into code, at least for the moment (Meyer, 2020). On the other hand, despite the idea that they are 'tamper-proof' and unamendable, there are some technical solutions to upgrade smart contracts (Ethereum, 2022), such as deploying intermediate smart contracts, which essentially are new contracts which use the 'delegate function' to get all the transactions redirected from the old version (Kotarani, 2019). Aside from being seemingly at odds with some of the benefits that standard smart contracts promise to offer, these solutions also come with significant risks and costs. These include the power of developers to modify smart contracts arbitrarily, without the parties' knowledge, increasing the complexity of the smart contract in question and thus the risk of critical flaws or making the smart contract vulnerable to malicious actors (Ethereum, 2022).

Second, some smart contracts require so-called oracles, that is, blockchain addresses through which relevant inputs for the contract are provided. Oracles act as bridges between what is on-chain (the contract) and off-chain (the data needed) in cases where the activation of the contract depends on external data (De Filippi et al., 2021). For example, in an insurance contract, oracles could be used to feed in data about the level of damages or nature of the event that caused them to trigger its execution. This need for oracles raises significant issues ranging from the trustworthiness of the oracle and its sources for data, to redress situations when the data collected are found to have been inaccurate (Egberts, 2017). Oracles create dependencies that can affect the entire blockchain and may also leave smart contracts in a situation in which they are forced to rely on centralised contract execution (Schär, 2021). The Proposal does not engage with the concept of oracles or any of these issues. It is unclear whether this is so because the Commission believes that smart contracts used in the Data Act context will not make use of oracles.

Third, smart contracts are also vulnerable to bugs and changes in the architecture on which they are based. Perhaps the most famous example is the attack on The DAO, which led to one-third of the funds raised by it being stolen and moved to a different account. This has been addressed through a controversial decision to 'hard-fork' the Ethereum blockchain, a radical change to the network's protocol, which made the transaction invalid, restoring almost the entire sum (Mehar et al., 2019). Smart contracts are also vulnerable to the network of miners that operate the underlying blockchain network on which they are based, which have the power to prevent the execution of a smart contract (De Filippi et al., 2021) or to influence it, as the hard-fork example shows. This is the 'miner extractable value' (MEV), which refers to the miner's ability to profit by exploiting smart contracts. MEV is deemed inevitable on public blockchains. If transparency is not in place, miners will lack the incentive to play by the rules. They will be motivated to abuse their possibility to alter the market conditions depending on their interests. These issues are partially addressed by the Proposal, through the inclusion of robustness as an essential requirement, understood as the capacity to avoid functional errors and withstand manipulation by third parties. However, this is much easier said than done. As The DAO example shows, smart contracts can have vulnerabilities and the way to ensure that they are addressed is not straightforward. Listing robustness as a requirement is insufficient if there is no specification of how it can be achieved. Here is where Article 30(5) of the Proposal could play a significant role, as it enables the Commission to request one or more European standardisation organisations to draft harmonised standards that satisfy the essential requirements.

Fourth, the immutability of the blockchain, while presented as one of its most significant advantages, also raises privacy issues. Other than being almost impossible to amend, smart contracts on the blockchain will be public and relatively easily accessible, giving away information about the involved parties and the scope of the agreement, unless the blockchain in question is private (Mohan, 2019). This raises significant privacy considerations that the Proposal should address. Unconventional transparency may also be a deterrent to innovation. For the reasons highlighted above, it is not in the interest of companies to disclose valuable information. Other than that, immutability can create rigidity and inflexibility in smart contracts (Chen & Bellavitis, 2019). Conversely, to avoid manipulation of network participants, immutability may contribute to transparency and distributed trust (Wieandt & Heppding, 2022). Yet, this applies to a limited extent as only users' addresses are disclosed, not their identities. Several protocols have been established in recent years that seek to solve the lack of privacy in smart contracts (Fernàndez-València, 2021). However, their effectiveness is questioned. Several different models have been suggested, each with shortcomings, including high costs and difficulties in applying widely (Goldfeder & Narayanan, 2018). Moreover, it is doubtful whether such solutions could be adopted at the scale required to achieve the vision expressed in the Data Act. Thus, despite these options, it remains problematic that the Proposal does not engage more with the issue of privacy in smart contracts.

Finally, the Proposal glosses over the critical issue of enforceability. The proposed regulation does not include details on how smart contracts will interact with domestic legal systems or how disputes will be solved where problems arise. At first glance, such a solution seems to be inspired by the well-established doctrine of procedural autonomy of the Member States (Halberstam, 2021), which relies on the constitutional principle of sincere cooperation (Article 4(3) TEU). That doctrine recognises that, in the absence of EU rules, it is for the municipal legal systems of each Member State to identify the mechanisms and tools to ensure the protection and enforcement of rights flowing from EU law.[2] In this respect, it does not come as a surprise that Chapter IX of the Proposal, dealing with Implementation and Enforcement, gives the Member States broad discretion in designating competent authorities and establishing penalties for infringements. However, this approach is likely to increase the risk of legal fragmentation, and places on the Member States the onerous burden of finding ways to make smart contracts workable within their legal systems, without providing potential solutions to the issues they raise. It would be helpful if the Commission indicated how smart contracts could interact with different domestic legal systems. Perhaps, one may follow the model of the Law Commission in the UK, which issued a report, in 2021, concluding that the law of England and Wales can accommodate smart legal contracts, without the need for statutory reform (Law Commission, 2021). Producing such an analysis would be an important step in helping and encouraging Member States to adopt smart contracts, paving the way for their wider adoption in the EU.

The Commission's partial reckoning with the issues raised by smart contracts shows a lot of enthusiasm to adopt Web3 solutions but insufficient commitment to address the shortcomings that make implementing them challenging. It is essential to acknowledge that, while smart contracts entail a significant improvement in digital ledger technologies, this is still a relatively novel environment. Thus, sound regulation is needed. In the Proposal, the Commission outlines a vision for better smart contracts, seemingly without considering the feasibility and desirability of this ambitious project. While the EU appears to be increasingly eager to join the conversation around Web3 solutions, animated by a strategy to be open to emerging digital trends, the difficulties of implementing such solutions successfully should not be underestimated. They must be addressed as soon as possible.

[2] *Rewe-Zentralfinanz eG and Rewe-Zentral AG v Landwirtschaftskammer für das Saarland*, case 33/76, EU:C:1976:188, para 5.

Declarations

Conflict of Interest The authors declare no competing interests.

References

Ante, L. (2020). *Smart contracts on the blockchain – A bibliometric analysis and review*. https://doi.org/10.2139/ssrn.3576393

Chen, Y., & Bellavitis, C. (2019). *Decentralized Finance: Blockchain Technology and the Quest for an Open Financial System.* https://doi.org/10.2139/ssrn.3418557

Czarnocki J. (2022). *Data Act Message – Legitimacy of the Data Processing and Consistency of Data Protection, KU Leuven Centre for IT & IP Law.* https://www.law.kuleuven.be/citip/blog/data-act-message-legitimacy-of-the-data-processing-and-consistency-of-data-protection/#:~:text=As%20a%20principal%20personal%20data,it%20is%20lawful%20and%20legitimate

De Filippi, P., Wray, C., & Sileno, G. (2021). Smart contracts. *Internet Policy Review 2021, 10(2).* https://doi.org/10.14763/2021.2.1549

Egberts, A. (2017). The oracle problem—An Analysis of how blockchain oracles undermine the advantages of decentralized ledger systems. https://doi.org/10.2139/ssrn.3382343

Ethereum. (2022). Docs, 'Upgrading Smart Contracts', 18 July 2022. https://ethereum.org/en/developers/docs/smart-contracts/upgrading/

European Commission. (2020). *A European Strategy for Data.* Available at: https://digital-strategy.ec.europa.eu/en/policies/strategy-data#:~:text=The%20Data%20Act%20is%20a,the%20European%20economy%20and%20society.

European Commission. (2022). Data Act: Proposal for a Regulation on harmonised rules on fair access to and use of data. Available at: https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rulesfair-access-and-use-data#:~:text=The%20Data%20Act%20aims%20to,to%20invest%20in%20data%20generation

Fernàndez-València R. (2021). *Private smart contract execution – A survey of existing proposals*. https://medium.com/iovlabs-innovation-stories/private-smart-contract-execution-7df89e28eb30

Goldfeder, S., & Narayanan, A. (2018). Private smart contracts. *Privacy Enhancing Technologies Symposium*. https://petsymposium.org/2018/files/hotpets/9-goldfeder.pdf

Halberstam, D. (2021). Understanding national remedies and the principle of national procedural autonomy: A constitutional approach. *Cambridge Yearbook of European Legal Studies, 2021*, 23. https://doi.org/10.1017/cel.2021.12

Kotarani, V. (2019). A beginners guide to blockchain smart contract. *Promact*. https://promactinfo.com/blogs/beginners-guide-to-blockchain-smart-contract/

Law Commission. (2021). *Smart Legal Contracts, Advice to Government*. Law Com No401. https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf

Mehar, M. I., Shier, C. L., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., ... & Laskowski, M. (2019). Understanding a revolutionary and flawed grand experiment in blockchain: The DAO attack. *Journal of Cases on Information Technology, 21*(1), 19–32. https://doi.org/10.4018/JCIT.2019010102

Meyer, O. (2020). Stopping the unstoppable - Termination and unwinding of smart contracts. *Journal of European Consumer and Market Law*, *17*.

Mohan C. (2019). State of public and private blockchains: Myths and reality. International Conference on Management of Data (SIGMOD '19), *Association for Computing Machinery*, New York, NY, USA, 404–411. https://ezproxy-prd.bodleian.ox.ac.uk:2102/10.1145/3299869.3314116

Schär, F. (2021). *Decentralized finance: On blockchain- and smart contract-based financial markets*. https://doi.org/10.20955/r.103.153-74

Wieandt, A., & Heppding, L. (2022). *Centralized and decentralized finance: Coexistence or convergence?*. https://doi.org/10.2139/ssrn.4046173