



(German Association of Crypto Registrars)

Berlin, 19 June 2023

Statement on the Mention of Smart Contracts in the Data Act

Against the background of the current trilogue negotiations on the Data Act, we would like to express our support for other industry initiatives such as the recently published Open Letter About Concerns and Proposed Refinements Regarding the Regulation of Smart Contracts in the Data Act (the ‘Open Letter’, <https://data-act.info/>). We share the overall concern that the current wording of the Data Act in relation to Smart Contracts could be interpreted too broadly. In a broad sense, the wording and the requirements under Article 30 could be understood to encompass all kinds of Smart Contracts used in the processing of data, beyond those for the specific purpose of sharing data sets under data sharing agreements.

There is no established definition of the concept of a ‘Smart Contract’, even though there are technical definitions under certain Blockchain protocols such as those compatible with the Ethereum Virtual Machine (EVM). As a result, different concepts have been described using the term over time. To our knowledge, the term has also not yet been formally defined in a legal act of the Union, despite being mentioned in certain provisions and recitals of individual legal acts, such as Article 7(4) of Regulation (EU) 2022/858 on a pilot regime for market infrastructures based on distributed ledger technology or Recital 96 of Regulation (EU) 2023/1114 on markets in crypto-assets. Against this backdrop, we advise against using the very specific context of the Data Act to provide a formal definition of this term for the first time, and also suggest avoiding the term in this context altogether. As an alternative to the term ‘Digital Contract’ proposed by the Open Letter, the description ‘tools for automating the execution of data sharing agreements’ as discussed for Article 28(1) could also be used.

Smart Contracts are widely used in both centralised and decentralised finance, in particular in the context of tokenisation, where they act as databases to record holdings in tokenised financial assets. However, such Smart Contracts are deployed on both public and private/permissioned DLT infrastructure. And even where the Smart Contracts are deployed on public DLT infrastructure, they might be considered to contain private or permissioned data records due to the specifics of the Smart Contract code which might, inter alia, involve encrypting certain parts of the data or include a permissions regime that assigns different permissions in relation to the data records to different parties. We therefore advise against any qualification of the requirements under Article 30 or the definition under Article 2(1)(16) limiting either to private(ly operated) or permissioned data records.

We thank you for attention to this matter and remain available to provide any clarification or further information on this matter. For that please reach out to d.wernicke@nyala.de.

Daniel Wernicke
Deputy Chairman