



# How Blockchain and Artificial Intelligence influence Digital Sovereignty

Martha Klare<sup>(✉)</sup> , Lisa Verlande , Maximilian Greiner ,  
and Ulrike Lechner 

Universität der Bundeswehr München, 85579 Neubiberg, Germany  
{martha.klare,lisa.verlande,maximilian.greiner,ulrike.lechner}@unibw.de

**Abstract.** Digital Sovereignty is an ascending field that is viewed from a society, politics and enterprise perspective. When considering the situation from an economic standpoint, it is still unclear how to understand the issue of what businesses can do to strengthen their Digital Sovereignty. Artificial Intelligence and Blockchain are disruptive technologies that have significant impact on Digital Transformation. This article studies the relationship between Digital Sovereignty and novel technologies, such as Artificial Intelligence and Blockchain. A quantitative survey with 163 respondents is the empirical basis of the analysis. We propose seven measures to strengthen Digital Sovereignty: preserve Data Sovereignty, address concerns and create awareness, define responsibilities, co-create transformation, expand expertise, promote freedom of choice and measurement criteria. The proposed measures support formulating a Digital Sovereignty strategy to ensure the vision, goals and requirements for balancing heteronomy and autarky in a self-determined manner.

**Keywords:** Digital Transformation · Digital Sovereignty · Blockchain · Artificial Intelligence

## 1 Introduction

In the context of Digital Transformation, Digital Sovereignty becomes a strategic goal. Considering the critical dependency on disruptive technologies such as the Internet of Things, Big Data, Virtual Reality, 5G, Artificial Intelligence (AI), or Blockchain, geopolitical issues and aspects such as independence, self-determination, trust and credibility are becoming more meaningful. The Digital Transformation leads to a change in Information Technology (IT) which makes the consideration of Digital Sovereignty indispensable [16]. An initial approach by researchers to break down Digital Sovereignty into dimensions leads to the distinction between the perspectives of state, economics and individuals as well as the relationships between each other [17]. Glasze et al. [19] and Ciriumaru [10] discuss challenges for central societal areas such as law, technology and ethics to express Digital Sovereignty. Researchers such as Fries et al. [17] or Pohle [30] make the first attempt to transfer the factors and influences of Digital

Sovereignty, as well as the linkages between the state, the economy and individuals into logical modeling. From an economic perspective, one way could be the exploration of growing technologies. Two growing technologies in the literature are AI and Blockchain [8, 22]. However, considering how to build or strengthen Digital Sovereignty with the selected technologies, it remains unclear how to interpret the answer. While there are many policy proposals for dealing with the promotion of Digital Sovereignty, concrete requirements for key technologies are scarce. Therefore, we decided to explore the impact of Blockchain and AI on Digital Sovereignty. Blockchain seems to contribute meaningfully to Digital Sovereignty due to its decentralization, multiple and distributed authorities, and tamper-resistance [3]. The link between AI research and Digital Sovereignty is obvious when constructing and designing trustworthy, credible and autonomous AI systems [33]. Furthermore, researchers adopting the Information Systems perspective are highly concerned with the issue of Data Sovereignty. For example, open networks [11] or remote evaluation [4] are proposed to ensure an appropriate level of Data Sovereignty. Our approach is to critically examine the impact of AI and Blockchain on Digital Sovereignty in organizations and their relationships. Furthermore, linking the concepts can help identify new potentials, research areas and directions in all three areas (AI, Blockchain and Digital Sovereignty) [20]. Finally, we create a list of measures to develop concrete recommendations for corporate management. Three research questions guide the analysis:

RQ1: What is the companies' state of Digital Sovereignty?

RQ2: How do AI and Blockchain support companies' sense of Digital Sovereignty?

RQ3: How to strengthen Digital Sovereignty?

Guided by these research questions, we investigate to what extent AI or Blockchain supports Digital Sovereignty and how Digital Sovereignty impacts the development and use of these technologies in companies. Therefore, this article contributes to the body of knowledge by outlining the impact of new technologies on enhancing corporate Digital Sovereignty based on empirical data.

This article is structured as follows. First, the research methodology is presented (Sect. 2), followed by the theoretical background (Sect. 3) that establishes a correlation between Blockchain, AI and Digital Sovereignty in terms of Digital Transformation. Section 4 presents the survey results, including the impact of AI and Blockchain on Digital Sovereignty. Finally, the conclusions and an outlook for further research are highlighted (Sect. 5).

## 2 Research Design

For our analysis, we employ a survey method guided by Lehmann et al. [23]. The following steps were taken within the study: determination of target group, creation of questionnaires, 19 conducted pretests, data collection and analysis. The survey uses semi-open and closed questions, one-dimensional scales and

Multiple-Choice-Questions. In addition, some of the questions were filter questions, ensuring that participants completed the questions they were most familiar with but that each question was answered multiple times. First, we carried out a statistical analysis following Muller et al. [28]. Network diagrams are used to depict and communicate our results. Finally, we create clusters to find similarities and proceed to the detailed analysis [28].

Data was collected over two months between July and August of 2022. The survey was conducted in Germany and targeted businesses and decision makers in Germany. We collected 163 person data sets (107 completed data sets) considering an error rate of 10%. The person data sets include 57 from small and medium-sized enterprises and 77 from large companies.

### 3 Theoretical Background

The following section provides definitional delimitation of the terms Digital Sovereignty, Blockchain and AI.

#### 3.1 Digital Sovereignty

Digital Sovereignty is a politically motivated goal and is often understood as a strategic balancing act between heteronomy and autarky [13]. States, companies and individuals want to be able to act in the digital world without cutting themselves off from others or becoming too dependent [31]. Thus, factors such as freedom of choice, independence in selecting IT products and the security of one's own country, citizen, or company play an important role in becoming more digitally sovereign [27]. Digital Sovereignty is not a fundamental value on its own. It is part of the values of liberal democracy, open competition policy and efforts toward greater digital sustainability, especially in German research [18].

Digital Sovereignty can help drive Digital Transformation by clarifying as state, business or individual how they want to use hardware or software and capabilities of others [27, 29]. In the digital sense, this means that politicians, researchers and decision makers in companies should increasingly ask themselves what technical, organizational and conceptual requirements for key technologies are needed to become truly more independent [12]. In the following section, the current state of research on Digital Sovereignty is expanded by subjecting two key technologies (Blockchain and AI) to the particular analysis. To broaden the understanding, information is provided on the extent company members believe that the implementation of AI or Blockchain can help strengthen Digital Sovereignty.

#### 3.2 Blockchain in the Digital Transformation

Blockchain is a kind of Distributed Ledger Technology and can be seen as the standard for digital transactions as B2B and B2C companies increasingly shift to the digital market [25]. Blockchain is seen as an accelerator of business processes, enabling reliable and secure transactions in various business areas to

be fully automated [1]. Because of increasing networking and connectivity, the technology allows agreements to be set up largely forgery-proof and in a transparent manner [5]. For us, Blockchain is a technical solution to manage data in a distributed infrastructure without a central instance in a traceable and tamper-proof way by consensus [36]. Moreover, Blockchain allows verifying transactions without a central instance in a transparent and trustworthy process [7]. Christidis and Devetsikiotis [9] proposed four main benefits of Blockchain technology: tolerance of node failures, a single view of events, data ownership without a central authority and transparent, verifiable, predictable as well as audible activities. Given these elements, we can assume a solid connection to Digital Sovereignty, as issues of ownership, transparency, trust, ethics and authority play a particular role. As outlined, the field of Blockchain and Digital Sovereignty holds significant research potential. To understand the current situation and derive assumptions, it is critical to explore recent adoptions, the state of the technology and the potential impact on Digital Sovereignty.

### 3.3 Artificial Intelligence in the Digital Transformation

As a result of digitalization, AI is experiencing a resurgence within research and various industries. This renewed upswing is due to the technological drivers within the Digital Transformation: improved computing capacities, faster connections and larger connectivity areas enable the usability of AI systems on a larger scale [6]. In this study, we define AI as a system that can make predictions and decisions based on algorithms and existing data sources through learning. AI algorithms focus on mapping three essential human cognitive abilities - learning, reasoning and self-reflection [32]. However, AI in the context of Digital Transformation also has much potential for debate. Particularly around ethical issues, risks, credibility, trust and even fairness, the question arises regarding how to achieve these. At these points, we see the connection to Digital Sovereignty, which becomes even more apparent when we look at the guiding principles of the European Union's AI Expert Group [15]: respect for human autonomy, harm avoidance, fairness and explainability. A deeper insight into the current use, purpose, obstacles and concerns of AI systems in enterprises is therefore crucial to set up AI systems for the future in a more digitally sovereign way. So, it is critical to uncover and profitably leverage the interfaces and goals between Digital Sovereignty and AI. One way to achieve more Digital Sovereignty in AI is through the recent machine learning approach called Federated Learning (FL), which we will discuss in our paper in Sect. 4.3.

## 4 Results

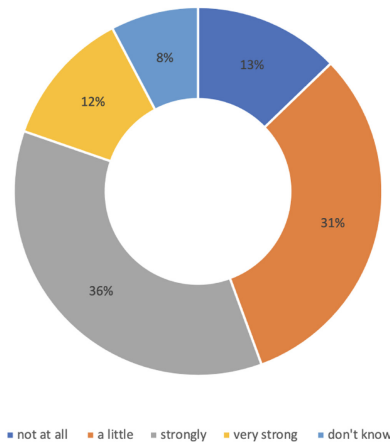
As the debate on Digital Sovereignty is still young, it is important to determine the level of awareness of the topic of Digital Sovereignty in companies and among decision makers. Therefore, we want to use the survey data to determine what measures have already been taken in connection with Digital Sovereignty.

## 4.1 Towards Digital Sovereignty in Enterprises

This section presents, analyzes and contextualizes the findings on the topic of Digital Sovereignty.

**Current State of Digital Sovereignty.** Employees and decision makers in companies are grappling with the idea of Digital Sovereignty. 79% of respondents state that they are aware of the topic and the interest in Sovereignty is strong to very strong at 67% (Fig. 1).

Would you describe your company as digitally sovereign? (in percent)

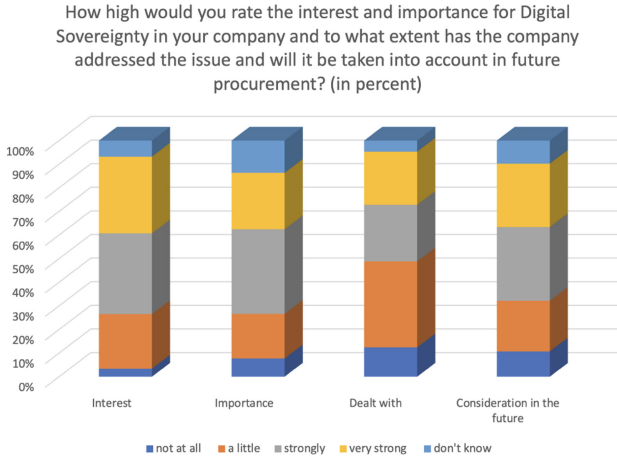


**Fig. 1.** Would you describe your company as digitally sovereign?

The importance of the topic to the companies is slightly lower. However, 60% of people rate the importance high to very high (Fig. 2).

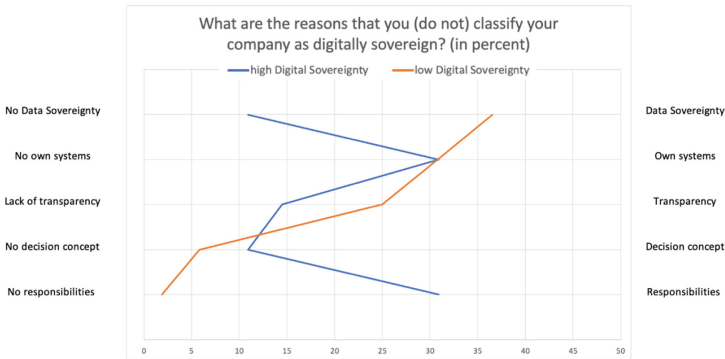
We asked how decision makers compare their state of Digital Sovereignty towards the competition and the result showed that the majority see themselves in the midfield compared with other companies. When asked which areas in companies are seen as already digitally sovereign, it does not seem clear to the respondents where Digital Sovereignty plays a central role in the company and why.

**Low Sovereignty vs. High Sovereignty in Companies.** The respondents were divided into two clusters based on their self-assessment regarding Digital Sovereignty in the company (group 1: low Digital Sovereignty, group 2: high Digital Sovereignty). It is striking that the proportion of companies from group 1 see low Data Sovereignty as the main reason for this (84%) and those who rate Digital Sovereignty in their own company as high (group 2), in turn, see accountability (31%), their systems (31%) and transparency (14%) as the reasons (Fig. 3). The results are consistent with Blossfeld et al. [2], who see selecting the



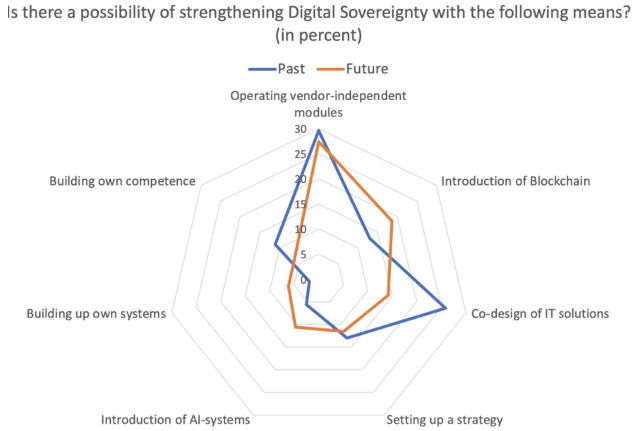
**Fig. 2.** How high would respondents rate the interest, importance, dependencies and the consideration of Digital Sovereignty for the future?

right people, right technologies and implementing the right processes as key drivers of Digital Sovereignty.



**Fig. 3.** What are the reasons that you (do not) classify your company as digitally sovereign?

**Lessons from the Past for Recommendations for Future Action.** We asked the respondents who considered their company to be digitally sovereign what measures their company has used in the past to strengthen its Digital Sovereignty. The results show that 30% of respondents have strengthened their Digital Sovereignty in the past by using vendor-independent modules. In addition, co-designing IT solutions (26%) and creating a strategy (13%) have also helped companies. Still, 63% of respondents said that their company had not paid



**Fig. 4.** Means of strengthening Digital Sovereignty

attention to ensuring that new technologies were digitally sovereign in their procurement in the past (Fig. 4). Now all participants were again asked to give their assessment. We asked what means they believe they can use to strengthen Digital Sovereignty in the future. According to the respondents, the goal of strengthening Digital Sovereignty in the future should be to gain more control over one's data, i.e., Data Sovereignty. Thus, 89% of respondents see the topic of Data Sovereignty as (very) important for strengthening Digital Sovereignty. The surveyed persons state that promoting research and development (34%) can significantly help companies to enhance Digital Sovereignty. In the future, employees and decision makers would use vendor-independent modules to strengthen their company's Digital Sovereignty (27%). Building and using Blockchain technology also appears to be a way to increase Digital Sovereignty in the future (up 6% points from the past). The importance of AI in enhancing Digital Sovereignty has increased by 5% points in the future compared to the past. Respondents believe that using strategic guidelines will help them better understand the complex subject (13%). As an alternative to the classic AI system, FL is seen by most respondents as a positive approach to strengthening Digital Sovereignty because only 10% denied that FL would help.

Obstacles to strengthening Digital Sovereignty, according to the respondents, are the main challenges in adapting the company's internal IT infrastructure (27%), information deficits (19%), lack of responsibilities (19%) and financing additional costs. The state is expected to support research and development (34%), more interoperability in national products (22%) and the development of a national data strategy (13%) to guide companies. Some respondents also mention expanding greater collaboration with EU countries (12%), more training opportunities (10%) and an open source strategy (5%).

**Expanding the Understanding of Digital Sovereignty.** As mentioned before, we understand Digital Sovereignty as a strategic balancing act between

heteronomy and autarky to successfully fulfill politically motivated goals. Our survey results verify the understanding of Digital Sovereignty of other researchers in regard to the factors freedom of decision, independence in selecting IT products, and compliance. 88% of our respondents see freedom of choice as an important factor for Digital Sovereignty, which shows that the assessments by Kagermann et al. [21], regarding the political goal of giving more weight to freedom of choice when addressing Digital Sovereignty, can be confirmed. Our survey results also supported Pohle and Thiel’s [31] assessment. They see independence in the choice of IT products as a central element of Digital Sovereignty, which 77% of the respondents can confirm. According to 70%, more guidance and compliance by the management itself is needed, which is in line with Weber [34], who sees compliance as a key factor to successfully integrating Digital Sovereignty.

In addition, we found that company-specific factors, such as the creation of transparency in IT architectures (77%), also play a major role. Last but not least, the decision makers see collaboration with stakeholders who share similar values (58%) and accessibility to the companies’ source codes (57%) as prerequisites for strengthening Digital Sovereignty.

## 4.2 Towards Artificial Intelligence and Blockchain in Enterprises

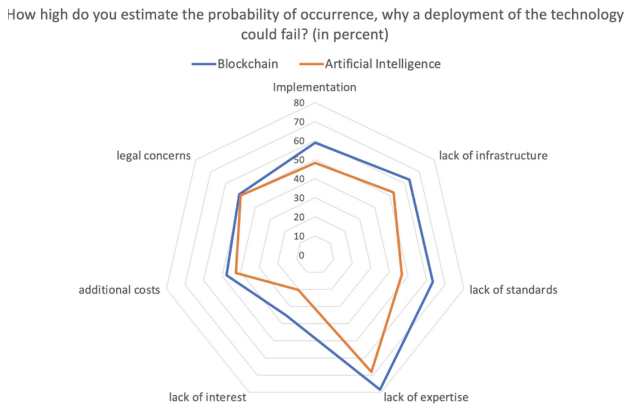
Regarding Blockchain and AI, we wanted to discover the awareness for the two technologies, their use cases, properties and purposes. In addition, respondents were asked whether their company works with the technologies and whether they would say Blockchain and AI would support Digital Sovereignty.

**Blockchain.** According to our survey, it can be assumed that 74% is not aware of Blockchain. In addition, we find out that many respondents are not sure whether their company invests in Blockchain projects. Thus, 30% stated that they do not know the status of Blockchain implementation in their company, while 33% noted that there are implemented and planned projects. This data can be directly related to Blockchain familiarity. The following three potential applications remain the most widely perceived: real-time certificate management (21%), cryptocurrencies (19%) and sensor data collection (16%). Blockchain, then, is best known for its tamper resistance (25%), the immutability of data (28%) due to the hash function, resilience (15%) and transparency due to the decentralized storage of information (15%).

**Artificial Intelligence.** Although AI is already used in many areas of daily life, more than 3/4 of respondents still say they have little or no knowledge about AI. As shown by the results, the best-known applications are intelligent systems (25%), voice control (15%) and text recognition (13%). However, it can be assumed here that while AI is known as a term, there is a significant lack of understanding of how AI works. In addition, 39% of respondents indicated that their company had implemented projects involving AI and another 21% of companies were already in the project planning phase. So, more than half of the respondents have already been confronted with AI in their daily work.



The cause for failure of Blockchain and AI projects has also been investigated. Although both technologies serve different purposes and are used in different areas, the picture is almost identical with regard to the question of what could be causes for failure in technology development (Fig. 5). Participants indicated that lack of expertise is the most common reason Blockchain or AI adoption fails. While interest in adopting AI and Blockchain is considered high, additional reasons include additional cost, legal concerns, implementation difficulty, lack of infrastructure and lack of standards (Fig. 5). Note that when asked about ways to strengthen Digital Sovereignty, Blockchain and AI are below 20% for both past and future (Fig. 4). Still, a later question revealed an approval rate of 54% (Blockchain) and 69% (AI) regarding positive support for Digital Sovereignty. The findings show a low understanding of how to strength strategic goals and underscore the importance of awareness and clear measurement criteria.



**Fig. 5.** Criteria of Blockchain and AI

### 4.3 Implications and Discussions of Artificial Intelligence and Blockchain for Digital Sovereignty

Digital Sovereignty is a strategic goal. To work towards this strategic goal, based on our data, we see the need to address the adoption of Blockchain and Federated Learning (Sect. 4.1). In addition, we have developed seven measures for consideration in a Digital Sovereignty strategy that pay attention to understanding, acknowledging and best implementing the vision, goals and requirements for a digitally sovereign enterprise. We use clusters and network diagrams to restructure the results, create codes and compare them to data from literature. We then further explored the data in two rounds of workshops within the research group, the first round consisting of the elementary collection of unstructured measures and the second for refinement and alignment. In doing so, our data analysis revealed that the following measures are relevant for future approaches.

**Preserving Data Sovereignty.** Preserving Data Sovereignty is a fundamental goal for respondents' approach to Digital Sovereignty (Fig. 3). FL is a new, decentralized approach first named by McMahan et al. [26], which shares models rather than data to protect user privacy. Over 90% of respondents can envision using FL instead of current machine learning methods to maintain Data Sovereignty (Sect. 4.1). Blockchain can also support Data Sovereignty due to the tamper resistance and immutability of the data. At the same time, one advantage of implementing Blockchain is the visibility that can be created within a supply chain, for example. While respondents cannot imagine sharing information with competing companies and thus losing a competitive advantage, sharing with suppliers and customers is entirely conceivable (Sect. 4.1). Blockchain can thus help create a secure and sovereign enterprise while maintaining Data Sovereignty. As Lu et al. [24] suggest, coupling the two technologies can have a game-changing effect by securing communications through Blockchain while maintaining Data Sovereignty through FL. Most respondents see the creation of transparency, fairness, and more Data Sovereignty as ways Blockchain and AI can help strengthen Digital Sovereignty, which is examined in Sect. 4.2.

**Co-create Transformation.** There seems to be a lot of interest in Digital Sovereignty in the context of Digital Transformation. However, it is also the task of corporate management to create and promote opportunities for further development. Although respondents do not see co-creation as a prerequisite for creating Digital Sovereignty in the future, respondents indicated that co-creation had been a key function in the past (Fig. 4). The availability of skilled labor is limited today, so knowledge pooling is an essential building block for transformation and Digital Sovereignty, so it seems to be a valuable factor for later projects. We attribute the weaker evaluation of this factor within the question about future projects to increase the understanding of the respondents, as here, the entire respondent group was asked and in relation to the past, only the persons who previously stated that projects have already been implemented (Fig. 4). Technologies like FL and Blockchain can support this journey by making collaborations secure and transparent while preserving an organization's expertise. In addition, realigning processes, adapting roles, breaking down old structures and forging new paths are critical governance milestones that help transform companies into digitally sovereign enterprises. This contrasts with an increased self-sufficiency idea that dominates the discussion in Dreo et al. [14].

**Expand Expertise.** The lack of expertise is a significant obstacle to successfully implementing a digitally sovereign strategy and incorporating Blockchain and AI (Fig. 5). Here, with company-wide sensitization, it is necessary to prepare specialists for the changes. This includes additional training and education measures, direct involvement in the ongoing structural change and creating a sovereignty strategy. In addition, this may involve encouraging skilled personnel to engage in their research and development as resources allow. Designing an open communication architecture, not only internally but also to external partners, research institutions and communities, as well as being open and flexible to

new ideas and willing to implement them. The emphasis is on active listening, especially for management.

**Encourage Freedom of Choice.** An important aspect of Digital Sovereignty is freedom of choice. When selecting services, products and systems, freedom of choice must continue to be promoted in the market. Monopolies or limited choice are barriers to leveraging Digital Sovereignty, as the respondents indicated in last part of Sect. 4.1. Integrating FL and Blockchain seems essential in supporting Digital Sovereignty by increasing the flexibility and interconnectivity of services as they imply a certain degree of autonomy and data protection.

**Define Responsibilities.** According to the statements of the respondents who already consider their company to be digitally sovereign, creating clear responsibilities is the key to a more digitally sovereign company (Fig. 1). The creation of responsibilities, roles and decision-making concepts is already discussed in governance approaches like Weill and Ross [35] and is seen as critical to the success of companies. In this way, information deficits, such as those that have been identified as barriers to the successful incorporation of Blockchain and AI, can be reduced (Fig. 5).

**Eliminate Concerns and Create Awareness.** To successfully implement a sovereignty strategy, concerns and less knowledge must be dispelled by a clearer picture of what Digital Sovereignty is and how it can be integrated. Digital Sovereignty, Blockchain and AI are all highly rated in terms of interest and significance by the respondents. In this context, more than half of the respondents even stated that they would describe their company as digitally sovereign, yet most respondents rate their familiarity with Digital Sovereignty as low to moderate (Fig. 2). At this point, it is clear that respondents perceive the term as value-creating and relevant but are unaware of what they associate with it and what the focus is in adoption and implementation. The gap between the respondents' importance and sense of Digital Sovereignty shows that creating and training employees can help to expand awareness and strengthen Digital Sovereignty in companies. Furthermore, raising awareness is crucial for successful integration when introducing Blockchain and AI, as the survey also showed knowledge gaps in this area (Sect. 4.2). Here, it is up to the research community to raise awareness of the technology by highlighting its added value.

**Measurement Criteria.** Within the previous sections, we could detect a certain skepticism and ignorance among the respondents. To mitigate this, we proposed awareness as one measure to create trust. Another measure could be the creation of measurement criteria. Political goals currently overshadow the concept of Digital Sovereignty. More business measurement approaches are needed to quantify the achievement of goals regarding this topic. Measurable and controllable criteria can help to make Digital Sovereignty more tangible and thus facilitate implementation for companies.

## 5 Conclusion and Outlook

Our findings show that the surveyed companies feel that Blockchain and AI - especially Federated Learning - can help strengthen Digital Sovereignty. Our paper extends the existing body of knowledge in that we conducted preliminary research on the impact of Blockchain and AI in the context of Digital Sovereignty. We expanded our understanding of Digital Sovereignty by identifying requirements for raising Digital Sovereignty from companies' perspective, making technological recommendations and proposing seven measures based on our data. From the survey and comparison with existing literature, we were able to formulate key requirements for a strategy to strengthen Digital Sovereignty. First, it is critical to develop awareness of data ownership and derive how to maintain control over data. In addition, companies need to make their employees more aware of Digital Sovereignty and Digital Transformation. This includes assigning roles and responsibilities within corporate governance to set a company up for Sovereignty. To act with digital confidence, it is also necessary to rethink and restructure outdated processes, roles and structures. Another measure to consider is the development and expansion of know-how. Additionally, selecting services, products, or systems is crucial to maintaining autonomy and protecting sensitive data. To establish tangible Digital Sovereignty for companies, there is a need for measurement criteria that can provide orientation for design. Finally, the main goal should be to formulate a strategy to ensure the comprehension of visions, goals and requirements for the specific company environment.

Based on the results, developing targeted measurement criteria for Digital Sovereignty and creating an initial strategy paper for companies are approaches that require further description, explanation and validation based on concrete design studies within further research projects.

**Acknowledgments.** The Project LIONS is funded by dtec.bw - Digitalization and Technology Research Center of the Bundeswehr which we gratefully acknowledge. We would also like to thank Bayern Innovativ for funding the project "Federated Learning Enhancing IT Security (FLEIS)" (DIK 0241\_2104\_0080). We thank our partners and fellow researchers and all study participants.

**Contributions** can be attributed to the coauthors as described below:

- Martha Klare addressed the volunteers with the survey and wrote the results section on Digital Sovereignty in Enterprises (4.1).
- Lisa Verlande wrote the section Towards Artificial Intelligence and Blockchain in Enterprises (4.2) and the Implications and Discussions of Artificial Intelligence and Blockchain for Digital Sovereignty (4.3).
- Maximilian Greiner added implications regarding the Discussions on Blockchain for Digital Sovereignty (4.3).
- The authors jointly designed the study and co-authored the introduction (Sect. 1), methodology (Sect. 2), theoretical background (Sect. 3) and conclusion (Sect. 5).
- Ulrike Lechner contributed to the research design, data collection, interpretation and revisions of the article.

## References

1. Akter, S., Michael, K., Uddin, M.R., McCarthy, G., Rahman, M.: Transforming business using digital innovations: the application of AI, blockchain, cloud and data analytics. *Ann. Oper. Res.* **308**(1), 7–39 (2020). <https://doi.org/10.1007/s10479-020-03620-w>
2. Blossfeld, H.P., et al.: *Digitale Souveränität und Bildung*. Waxmann, Gutachten. Münster (2018)
3. Bons, R.W.H., Versendaal, J., Zavolokina, L., Shi, W.L.: Potential and limits of Blockchain technology for networked businesses. *Electron. Mark.* **30**(2), 189–194 (2020). <https://doi.org/10.1007/s12525-020-00421-8>
4. Bruckner, F., Howar, F.: Utilizing remote evaluation for providing data sovereignty in data-sharing ecosystems. In: 54th Hawaii International Conference on System Sciences (2021). <https://doi.org/10.24251/HICSS.2021.842>
5. Buhl, H.U., Schweizer, A., Urbach, N.: Blockchain-Technologie als Schlüssel für die Zukunft. *Zeitschrift für das gesamte Kreditwesen* **12** (2017)
6. Calp, M.H.: The role of artificial intelligence within the scope of digital transformation in enterprises. In: *Advanced MIS and Digital Transformation for Increased Creativity and Innovation in Business*. IGI Global (2020)
7. Carayannis, E.G., Christodoulou, K., Christodoulou, P., Chatzichristofis, S.A., Zinonos, Z.: Known unknowns in an era of technological and viral disruptions-implications for theory, policy, and practice. *J. Knowl. Econ.* **13**(1), 587–610 (2022)
8. Chatterjee, R., Chatterjee, R.: An overview of the emerging technology: blockchain. In: 3rd International Conference on Computational Intelligence and Networks (CINE). IEEE (2017)
9. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the Internet of Things. *IEEE Access* **4** (2016). <https://doi.org/10.1109/ACCESS.2016.2566339>
10. Circiumaru, A.: The EU's digital sovereignty-the role of artificial intelligence and competition policy. SSRN: 3831815 (2021)
11. Dalmolen, S., Bastiaansen, H., Kollenstart, M., Punter, M.: Infrastructural sovereignty over agreement and transaction data ('metadata') in an open network-model for multilateral sharing of sensitive data. In: 40th International Conference on Information Systems, ICIS 2019. Association for Information Systems (2020)
12. Bundesregierung, D.: *Datenstrategie der Bundesregierung: Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum*. Bundeskanzleramt, Berlin (2021)
13. Diekmann, G.: *Digitale Souveränität: Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa*. Bitkom, Berlin (2015)
14. Dreo, G., Eiseler, V., Gehrke, W., Helmbrecht, U., Hommel, W., Zahn, J., et al.: *Europäische Digitale Souveränität: Weg zum Erfolg?—Ein Bericht zur Jahrestagung CODE 2020*. *Zeitschrift für Außen-und Sicherheitspolitik* **13**(4), 399–404 (2020)
15. Europäische Kommission, Generaldirektion Kommunikationsnetze, Inhalte und Technologien Kommission: *Ethikleitlinien für eine vertrauenswürdige KI*. Publications Office (2019). <https://doi.org/data.europa.eu/doi/10.2759/22710>
16. Friedrichsen, M., Bisa, P.J. (eds.): *Digitale Souveränität*. Springer Fachmedien Wiesbaden, Wiesbaden (2016). <https://doi.org/10.1007/978-3-658-07349-7>, <http://link.springer.com/10.1007/978-3-658-07349-7>
17. Fries, I., Greiner, M., Hofmeier, M., Hrestic, R., Lechner, U., Wendeborn, T.: Towards a layer model for digital sovereignty: a holistic approach. In: *Proceedings of the 17th International Conference on Critical Information Infrastructures Security (CRITIS 2022)*. Springer (2022). in preparation

18. Fritzsche, K., Pohle, J., Bauer, S., Haenel, F., Eichbaum, F.: Digitalisierung nachhaltig und souverän gestalten. DINA, Positionspapier, CO (2022)
19. Glasze, G., Odzuck, E., Staples, R. (eds.): Was heißt digitale Souveränität?: Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter. Transcript Verlag (2022)
20. Hartmann, E.A.: Digitale Souveränität: Soziotechnische Bewertung und Gestaltung von Anwendungen algorithmischer Systeme. In: Digitalisierung souverän gestalten II. Springer Vieweg, Berlin, Heidelberg (2022)
21. Kagermann, H., Streibich, K.H.: Digitale Souveränität - Status quo und Handlungsfelder. acatech IMPULS (2021)
22. Lee, J., Suh, T., Roy, D., Baucus, M.: Emerging technology and business model innovation: the case of artificial intelligence. *J. Open Innov. Technol. Market Complex.* **5**(3), 44 (2019)
23. Lehmann, D.R., Gupta, S., Steckel, J.H., Gupta, S.: *Marketing Research*. Addison-Wesley Reading, Boston (1998)
24. Lu, Y., Huang, X., Dai, Y., Maharjan, S., Zhang, Y.: Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Trans. Ind. Inf.* **16**(6), 4177–4186 (2019)
25. Massaro, M.: Digital transformation in the healthcare sector through blockchain technology. *Insights Acad. Res. Bus. Dev. Technovation*, 102386 (2021)
26. McMahan, B., Moore, E., Ramage, D., Hampson, S., Arcas, B.A.: Communication-efficient learning of deep networks from decentralized data. In: *Artificial Intelligence and Statistics*. PMLR (2017)
27. Merkel, A., Frederiksen, M., Marin, S., Kallas, K.: Letter to the President-Digital Sovereignty. European Commission, Berlin (2021)
28. Müller-Böling, D., Klandt, H.: Methoden empirischer Wirtschafts- und Sozialforschung. Eine Einführung mit wirtschaftswissenschaftlichem Schwerpunkt **3** (1996)
29. Philipp, U.: Schriftliche Frage an die Bundesregierung (2022). <https://mdb.anke.domscheit-berg.de/wp-content/uploads/2022/03/1-76-Domscheit-BergGeschwaerzt.pdf>
30. Pohle, J.: Digital sovereignty. a new key concept of digital policy in Germany and Europe. Konrad-Adenauer-Stiftung, Berlin (2020)
31. Pohle, J., Thiel, T.: Digitale Souveränität – Von der Karriere eines einenden und doch problematischen Konzepts. In: *Der Wert der Digitalisierung: Gemeinwohl in der digitalen Welt*. Bielefeld: Transcript Verlag (2021)
32. Shinde, P.P., Shah, S.: A review of machine learning and deep learning applications. In: *4th International Conference on Computing Communication Control and Automation (ICCubeA)*. IEEE (2018)
33. Vogt, R.: Digitale Souveränität und Künstliche Intelligenz für den Menschen. In: *Digitalisierung souverän gestalten*. Springer Vieweg, Berlin (2021)
34. Weber, H.: Digitale Souveränität. *Informatik Spektrum* 1–12 (2022)
35. Weill, P., Ross, J.W.: *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Harvard Business Press, Boston (2004)
36. Xu, M., Chen, X., Kou, G.: A systematic review of blockchain. *Fin. Innov.* **5**(1), 1–14 (2019). <https://doi.org/10.1186/s40854-019-0147-z>