European Review of Digital Administration & Law - Erdal
2021, Volume 2, Issue 2, pp. 31-36
ISSN 2724-5969 - ISBN 979-12-5994-752-9 - DOI 9791259947529 04

The Use of Blockchain in Public Administration*

Lisa Wiese
(Research Fellow, Chair for Public International Law and Public Law at the Leipzig University)

ABSTRACT The potential fields of application for blockchain technology are many and varied. While the technology gained recognition primarily through its use in cryptocurrencies – such as Bitcoin or Ethereum –and its impact on the financial sector, there are far-reaching opportunities for the application in industry, commerce and also public administration.The German federal government wants to make Germany one of the leading locations for blockchain technology and issued a strategy on how to fully exploit the potential of the technology as an innovation driver. In this context, the federal government sees a potential to sustainably transform and influence public administration. The strategy explicitly formulates a wide range of application possibilities like registry management, digital identity and data verification. Therefore, Blockchain technology could replace institutional trust with self-managed and autonomous transparency.
The article briefly describes the technology of the blockchain and its essential features (1.), gives examples of the potential use of blockchain in public administration in Germany (2.) and assess legal challenges and effects with regard to data protection and constitutional law (3.).

1. *What is Blockchain Technology?*

The blockchain is a complex and multilayered informatic construct. It is not a completely new technology, but an innovative combination of existing concepts. In simplified terms, the blockchain is a decentralized database in which data blocks are symbolically strung together in a chain and stored distributed in a network[1]. It can be compared to a database, which belongs to no one and at the same time belongs to everyone, since a copy is stored on every connected computer. In this way, a blockchain ensures an exchange of information, values and goods of any kind without having to resort to intermediary institutions. The essential features of a blockchain, which make the definition a little more understandable, include the following.

1.1. *Decentralized*

Blockchain technology's development was based on the vision of a system with decentralised distribution, one that is to take over from central organisational units and is to make transactions possible directly between the given network's participants (peer-to-peer networks). Blockchain represents a secure and decentralized framework for transaction processing. The ability to record facts and data with built-in protection against malicious interference creates undeniable advantages over other distributed data processing and storage systems, thereby promising to save us from intermediaries[2].

1.2. *Immutability*

In previous data transactions, only an identical copy was transmitted to the recipient[3]. If it is to be ensured that the sender no longer has the corresponding data record as a result of the transmission process, verification by an intermediary such as a bank or another administrative office would be required. To enable the blockchain to dispense with the intermediation of intermediaries, all transactions of a data record are archived chronologically on several computing units connected to the network. A cryptographic process is used to verify and prove the effectiveness of data transmission: when a new data block is formed and linked to the transaction history, a computer solves a mathematical problem and the result is confirmed by other computers participating in the network. The decentralized consensus

* Article submitted to double-blind peer review.
This article uses the term 'blockchain' as a synonym for "distributed ledger technologies".
Refer to https://www.bundesregierung.de/breg-de/themen/digitalisierung/blockchain-strategie-1671902.
Refer also to https://www.euractiv.de/section/innovation/news/deutschlands-steiniger-weg-zur-blockchain-nation/.

[1] See https://legislature.vermont.gov/statutes/section/11-/025/04173.

[2] C. Welzel, K.-P. Eckert, F. Kirstein and V. Jacumeit, *Mythos Blockchain: Herausforderung für den öffentlichen Sektor*, Berlin, Kompetenzzentrum Öffentliche IT, 2017, 3, 17.

[3] F. Faust, *Zivilrechtliches Gutachten zum 71. DJT 2016: Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?*, Munich, Beck, 2016, 1.

process is highly tamper-proof and provides an algorithmic guarantee of correctness.

1.3. *Transparency*

All accesses and interactions in a blockchain are distributed to all participants in the blockchain network and are thus openly visible. No information can be changed or deleted, but only new information about the change of circumstances can be stored, so that up to the origin every change and every access in the blockchain is traceable for everyone[4].

1.4. *Anonymity*

While all accesses and activities of the participants in the blockchain are completely transparent and can be traced by anyone, the users behind them are only represented by cryptographically encrypted rows of numbers. In the blockchain, users are only visible with a "public key" and it is not possible to draw conclusions about a person from an individual transaction. Public distributed decentralized networks ultimately work with asymmetric encryption. Users have a public address, a kind of account number, and a "private key". The "private key" gives access to the user's public address. Basically, the "private key" is the personal password[5]. Depending on the type of blockchain, it is very difficult and sometimes even impossible to determine the real identity of a participant. Only by analyzing all transactions that have been made from a public address, it may be possible to draw conclusions about individuals or organizations[6].

In summary Blockchains are decentralized, digital registers that can offer a high degree of data integrity and trustworthiness through cryptographic processes and decentralized storage. The technology could contribute to the modernization of registers and the digitization of documentation processes and drive the automation of processes[7].

2. *Applying blockchain technology in public administration*

In many cases today, actors of the public sector perform the role of intermediaries. The public administration maintains registers to document ownership structures, while notaries, through their special position of trustworthiness, ensure ownership transfers. In addition, the state serves in many situations as a trusted third party, such as when it comes to confirming identities of persons or things or verifying the authenticity of documents. Therefore, the use of blockchain technology in many areas of public administration is quite conceivable.

The spectrum of current discussion for potential application areas in public administration ranges from the mapping of digital identities to transparency and openness, publicly maintained registers and management of ownership, proof of origin, verification and confirmation services, e-payment as well as securing electronic elections. In the following, only the most relevant application possibilities will be discussed, for which pilot projects have already been started or for which there is at least particularly promising potential for use.

2.1. *Digital Identity (eID)*

Prerequisites for the creation of digital administrative services are digital identities for individuals. Digital identities act as an important foundation for the use of digital services and networking, because they make communication, data exchange and transactions possible.

With the Online Access Act (Onlinezugangsgesetz) the federal, state and local governments are obliged to offer their administrative services digitally by 2022. Administrative portals of the federal government, the states and the municipalities will be technically linked in order to provide uniform access to all digital services offered by public administration. User accounts will be provided for citizens and companies in the

[4] See footnote 5, 17.

[5] This is a strength of the new technology, but also a disadvantage, since there is no central authority that can communicate or even reset the password in case it is forgotten According to a study by the Chain lysis, about 13-22% of all coins created so far (about 2.3 - 3.7 million coins) are lost forever because, among other things, the "private key" has gone missing, cf. https://blog.chainalysis.com/reports/money-supply. Especially in early years of Bitcoin, when the price was still in the penny or single-digit dollar range, according to Chain lysis, many users paid little attention to securing their Bitcoin holdings. It is likely that assets lie on many old hard drives or forgotten USB sticks. See for example: https://www.spiegel.de/wirtschaft/james-howells-der-mann-der-100-millionen-dollar-im-muell-sucht-a-1184783.htm.

[6] See footnote 5, 17.

[7] Refer to https://www.bmwi.de/Redaktion/DE/Downloads/B/bekanntmachung-umsetzung-blockchain-strategie.pdf?__blob=publicationFile&v=4.

portal network. Up to now the means of identification are a combination of user name and password and the online ID function.

It would also be possible that a connection between this user account and blockchain technology could create the basis for carrying out and recording user-to-user transactions in digital administrative services.

In Germany it is currently examined whether these blockchain based digital identities offer the prospect of a clear added-value compared to existing solutions, and whether they can be structured in a way that satisfies data protection law's requirements. In addition, the structuring must regard practicability, user-friendliness and the guaranteeing of autonomy in terms of information (informationelle Selbstbestimmung). Furthermore, the Federal Government is examining in various public-administration procedures, whether and to what extent, it is possible to accept derived digital identities from the private sector, either for public-administrative procedures or respectively for certain legal transactions[8].

The first prototypes for public digital identities already exist in Estonia and Switzerland. The E-Government Programs of these countries are becoming a showcase for many other countries with regard to blockchain-based initiatives. The Swiss city *Zug*[9] developed a blockchain-based digital ID with which citizens have access to various public services like bike rental, parking management, book lending from libraries and more.

Since 2015 the Baltic state has been offering blockchain-based administrative services with its e-residency program (e-Estonia)[10]. The program combines digital identities with a blockchain-based public authority system ("X-Road"). As a result, all 2.400 public services of Estonia[11] can be accessed digitally by its citizens (except from marriage, divorce and house purchase).

2.2. *Transparency and Openness*

The public sector is increasingly faced with the challenge of making its activities and decisions more transparent and comprehensible. With open data projects, the federal government[12] and local authorities are making their own data easily accessible and open to the public. Even at European level an online portal for open data has been made available[13].

Blockchain technology can take transparency performance to a new level of quality. For example, the origin and authenticity of data can be secured by a blockchain, which would increase confidence in the correctness, or source of the data itself[14].

Another field of application in this area are public budgets. Revenues and expenditures of public budgets can be made more transparent by storing a transaction in a blockchain. Such a concept could also be applicable to international aid[15] or donation financing, by providing information on how and for what the funds are used. This could help to prevent misuse and at the same time reduce bureaucracy.

2.3. *Public Register and Verification*

One of the main tasks of public administration is to grant, modify, transfer and document rights. For example, public administration offices register who owns a car, who is married to whom, who has received a place in a kindergarten, who owns a piece of land, who has a driver's license, or who is allowed to set up an advertising system

[8] See https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Projekte_Umsetzungsphase/projekte_umsetzungsphase.html.
[9] https://www.stadtzug.ch/newsarchiv/431448.
[10] Jameson, Hudson, Hard Fork No. 4: *Spurious Dragon – Ethereum Blog*, 16 March 2017, https://blog.ethereum.org/2016/11/18/hard-fork-no-4-spurious-dragon/.
[11] See https://www.eesti.ee/et.

[12] Refer to https://www.bundesregierung.de/breg-de/suche/open-data-strategie-1939808.
[13] See https://data.europa.eu/de.
[14] J. Smith, J. Tennison, P. Wells, J. Fawcett and S. Harrison, *Applying blockchain technology in global data infrastructure*, Open Data Institute, 2016, see http://theodi.org/technical-reportblockchain-technology-in-global-data-infrastr.
[15] The Federal Ministry for economic Cooperation set up the project "TruBudget": a digital working platform for the transparent and secure implementation of public investments in developing countries, which is technically based on a blockchain. The platform is up and running in four Countries. Brazil has been using "TruBudget" for 2 years as part of the Amazon Fund. In Georgia since July 2020, two projects with a volume of around 200 million have been documented on "TruBudget" since July 2020. Further FC projects in Ethiopia and Burkina Faso will follow.
"TrueBudget" transparency through blockchain: see https://www.bmz.de/de/entwicklungspolitik/digitalisierung/ziele-und-schwerpunkte/ziel-04-12216.

in the street. These rights are well documented in registers.

All these registers store data on persons or institutions and document changes over time. Managing and storing various rights in registers are one of the main tasks of public administration offices. Keeping these public registers on a blockchain seems quite obvious, as the blockchain with its verifiable, transparent documentation of transactions is already very similar to a classic register[16]. However, proposals that see blockchain as a quasi-substitute for registers should be viewed critically[17]. It limits the view of the actual potential of the technology for public administration: this lies much more in its use as a digital system for certification and verification of rights rather than in the abolition of registers.

With help of the blockchain it would be possible to manage a certification system (excerpts from the registers, e.g. birth certificate) in a more simplified way[18]. The citizen who has to provide a certificate could give a temporary permission to check whether corresponding rights are available to the recipient, for whom the proof is needed[19]. Each query in the blockchain is automatically logged in order to create transparency and security for the parties involved.

2.4. *Elections*

Another potential application of blockchain is e-voting (electronic voting) or even I-voting (voting over the Internet). In such a context, each voter generally receives a coin (or token) that represents his or her vote. Each candidate gets a receiving address (comparable to a wallet). The election itself is represented by a transaction of the coin to the candidate's receiving address.

While there are concerns for blockchain-based parliamentary elections[20], from a state organization law (Staatsorganisationsrecht) perspective, elections via blockchain would be possible. The considerations made in this regard include tangible benefits such as immediate overview of votes, high data integrity and benefits like an increase in voter turnout[21]. If a blockchain-based election system is appropriately designed, no violation of the principles of electoral law codified in Article 38 para. 1 of the German Constitution[22] is evident. On the contrary, a blockchain-based electoral system could violate the principal of publicity according to Art. 38 (1) and Article 20 para. 1 and 2 of the German Constitution. According to this principal, the essential parts of an election must be publicly auditable. This means that every citizen must be able to reliably understand the central step of the election process. This puts blockchain technology due to its technical complexity in a difficult position[23]. In a decision on the constitutionality of voting computers, the German Constitutional Court stated that every voter must be able to reliably convince himself of the legality of the election[24]. In this respect, the Constitutional Court further stated that no information technology knowledge may be necessary for the comprehensibility of the voting process[25]. However, it can be objected that the data collection and data processing mechanisms of digital information technologies are generally and fundamentally beyond actual perception. It is therefore appropriate to be sceptical as to whether technical comprehensibility for the entire voters represents a legitimacy of the digital state. The BVerfG is obviously not quite serious about this itself since it has made the proposal that electronic voting machines should additionally print out a paper record/protocol of the votes[26]. Moreover, printing out the votes would not improve the technical understanding and verification of the election, because it would still not be possible to verify whether the printed votes

[16] A. Berger, *Blockchain – Mythos oder Technologie für die öffentliche Verwaltung*, in *Deutsches Verwaltungsblatt*, vol. 132, n. 20, 2017, 1271.
[17] D. Rehfeld, *Blockchain in der öffentlichen Verwaltung* in T. Klenk, F. Nullmeier and G. Wewer (eds.), *Handbuch Digitalisierung in Staat und Verwaltung*, Wiesbaden, Springer VS, 2020, 68.
[18] D. Rehfeld, *Grundlagen einer möglichen Infrastruktur*, in *www.egovernment-computing.de*.
[19] See Footnote 20, 22.
[20] W. Prinz and A. Schulte (eds.), *Blockchain and Smart Contracts*, Fraunhofer-Gesellschaft, 2018, 29; Fn. 5, 22.
[21] P. Boucher, *What if blockchain technology revolutionized voting?*, European Parliament Research Service, 2016, see: http://www.europarl.europa.eu/thinktank/de/document.html?reference=EPRS_ATA(2016)581918.
[22] "Members of the German Bundestag shall be elected in general, direct, free, equal and secret elections".
[23] J. Susskind, *Decrypting Democracy: Incentivizing Blockchain Voting Technology for an Improved Election System*, in *San Diego Law Review*, 2017, vol. 54, 785, 814.
[24] *BVerfG* MMR 2009, 317.
[25] *BVerfG* MMR 2009, 318.
[26] *BVerfG* MMR 2009, 319.

corresponded to the actual votes. It remains to be seen whether a renewed attempt will be made to digitize the voting process.

2.5. *European Blockchain Service Infrastructure (EBSI)*

Blockchain technology is characterised by a decentralised infrastructure on which the most diverse range of applications can be provided. With regards to transnational and cross-sectorial interoperability of the blockchain, the demand for a public infrastructure used for blockchain applications arises. This blockchain infrastructure should support companies or organisations in developing specific applications. State infrastructure activities are associated not only with the hope of setting standards for interoperability but also for establishing governance structures for decentralised networks.

The European public sector is building its own blockchain services infrastructure, which should soon be interoperable with private sector platforms[27]. European Blockchain Service Infrastructure (EBSI) focuses on a small number of specific use cases (applications), and plans to expand over time.

Through the European Blockchain Partnership, the German government is actively participating in the development of the European Blockchain Services, which will also be used to provide EU-wide administrative services. The first use cases will go live shortly. At the national level, work is underway on a national Blockchain infrastructure for the public sector as part of *Govdigital*[28]. Some administrative solutions based on blockchain technology have already been piloted, including to support inter-agency communication and collaboration in the asylum process or to transparently and securely implement public investments in developing countries. Other solutions are currently still being worked on, such as an electronic vehicle record (eFA), more efficient customs valuation of e-commerce transactions with third countries, or digitally verified competency certificates and job references[29].

3. *Legal challenges and other effects*

Many of the internationally discussed application scenarios in the public sector are accompanied by a number of new challenges. Building and running a blockchain is not trivial and requires experienced professionals, including cryptologists and computer scientists. In addition to a variety of open technical points, there are also fundamental questions involved. Classic intermediaries create trust through organizational measures. Intermediaries in the public sector are subject to special requirements with regard to correctness and trustworthiness. Blockchain technology replaces this organisational trust with confidence in technology and its cryptographic processes. In this context, it has to be considered in each case whether the use of blockchain is reasonable and sustainable in the long run.

Emphasis was given to potential efficiency increases, resulting from simplified data exchange across horizontal and vertical administration levels, reduced duplication of data, and lower transaction costs. There was also a description of the technology's potential with regard to transparency, participation and traceability of administrative processes. However, the demonstrated advantages of the blockchain come with legal barriers regarding current data protection requirements[30].

Immutability of stored data and transparency of blockchain coupled with its temporal unlimited traceability are in contradiction to essential basic principles of current data protection law. This concerns in particular the right of deletion (Art. 17 DSGVO in conjunction with § 35 BDSG), correction (Art. 16 DSGVO), blocking (Art. 18DSGVO) and information (Art. 15 DSGVO in conjunction with § 34 BDSG).

Various approaches are being discussed in order to eliminate legal concerns. Consideration is given to reducing the right to deletion for complex, decentral organized IT systems in favour of a right to sufficient protective measures, in order not to jeopardize the innovation potential of blockchain technology[31].

However, the conflicts under data

[27] See https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure.
[28] See https://www.govdigital.de/themen-leistungen/blockchain.
[29] See https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure.
[30] Basic Data Protection Regulation (DSGVO) and the national Federal Data Protection Act.
[31] M. Martini and Q. Weinzierl, *Die Blockchain-Technologie und das Recht auf Vergessenwerden*, in *Neue Zeitschrift für Verwaltungsrecht*, vol. 36, n. 17, 2017, 1251, 1258.

protection law could also be resolved on a technological or conceptual level. One approach is to store the personal data permanently encrypted on the blockchain. At the same time the user can give selective permission to a third-party to access the data[32].

An expert opinion by the Federal Office for Migration and Refugees on the use of blockchain technology in asylum procedures concludes: "The planned use of a *permissioned blockchain* is generally permissible under data protection law. However, there is a compelling need for adjustment with regard to the development of a deletion concept for the personal data stored in the blockchain"[33].

At the same time the question must be asked as to whether the use of the blockchain technology makes any sense at all, if technical adjustments have to be made in the specific application.

Another open issue is the question of regulation and the role of the State. The challenge for regulation lies in the decentralized nature of the blockchain approach. Classic regulatory mechanisms reach their limits, when contact persons and responsibilities are not given. Therefore, with regard to the blockchain, there is a demand for "state regulatory resistance". Others disagree because there are also participants in blockchain networks who play a key role and bear more responsibility (like miners or traders for example) than other participants. Thus, addressees of regulation can certainly be identified. However, the global nature of the network makes it difficult to regulate on a national level[34].

4. *Future Perspectives*

Blockchain technology with its outlined characteristics of security, immutability and decentralization, can represent a thoroughly revolutionary development for public administration. At the same time, the technology brings complex challenges. The computing power required to operate a blockchain raises questions about energy efficiency. So far, reliable estimates of the climate impact of upscaling blockchain technology are lacking and research is still needed in this regard. In addition, policymakers are faced with the task of examining whether the current framework conditions do justice to the protection of people when exchanging sensitive data. It should be taken into account that blockchains represent a technological solution to certain trust problems that arise at very different points in administration. But not every problem necessarily needs a blockchain solution. Unlike other states without a functioning administration and a general lack of trust in public authorities, for Germany it is necessary that a serious advantage can be identified to justify a change in the existing system. Germany is equipped with public state infrastructure which is efficient and the risk of manipulation is limited – at least at first glance.

However, demographic change and the associated shortage of skilled workers, our state structures are in danger. It is an open secret that the public sector is affected by the shortage of skilled workers and will be affected to an even greater extent in the future[35]. In this respect, serious consideration should be given to the possibilities of compensation with the help of blockchain technology

[32] N. Guggenberger, *Datenschutz durch Blockchain – eine große Chance*, in *Zeitschrift für Datenschutz*, vol. 7, n. 2, 2017, 49.

[33] T. Hoeren adn J. Baur, *Datenschutzrechtliche Zulässigkeit der Übermittlung von Informationen über Migrantenzwischen öffentlichen Stellen mittels einer „permissioned Blockchain*", 38: https://fragdenstaat.de/anfrage/gutachten-blockchainbamf/302470/anhang/ifg_gutachten_blockchain.pdf.

[34] Refer to footnote 5, 24.

[35] In 2030 the public sector will not be able to fill 816.000 positions due to a lack of qualifies applicants. See study by Price Waterhouse Cooper "Shortage of skilled workers in the public sector", 2017, 39: https://www.pwc.de/de/branchen-und-markte/oeffentlicher-sektor/fachkraeftemangel-im-oeffentlichen-dienst.html.