DOSSIÊ

Artificial intelligence, data protection, and human rights

Editors
Fernanda Carolina de Araújo Ifanger e Lucas Catib De Laurentiis

Conflict of interest
The author declare they have no conflict of interests.

Received
October 29, 2024

Approved
October 29, 2024

REVISTA DE DIREITOS HUMANOS
E DESENVOLVIMENTO SOCIAL

Enforcement of data subject rights of the GDPR in blockchains

Cumprimento dos direitos dos titulares de dados do RGPD em blockchains

Frédéric Michel[1]

[1] Attorney at law at Scheja & Partners GmbH & Co. KG, Bonn, Germany; participant of the Master of Laws Program "Information Technology and Law" at Saarland University. Saarbrücken, Germany. E-mail: <frederic.michel@web.de>.

How to cite this article: Michel, F. Enforcement of data subject rights of the GDPR in blockchains. *Revista de Direitos Humanos e Desenvolvimento Social*, v. 5, e2414797, 2024. https://doi.org/10.24220/2675-9160v5a2024e14797

Abstract

The article examines whether and how the rights of data subjects under the European General Data Protection Regulation (GDPR) can be enforced within blockchain systems. Given the technical characteristics of blockchains, enforcing these rights appears to be challenging, or even impossible, particularly concerning the right to erasure, which is fundamentally impacted by the immutability of blockchain technology. This article presents the technical features of blockchains and explains the issues associated with enforcing rights of data subjects. Additionally, it investigates which actors involved in blockchain networks should be regarded as data controllers, thereby identifying the parties to whom data subjects can direct their requests. Finally, it discusses potential technical and organizational approaches to resolve the conflicts identified.

Keywords: Blockchain; data protection; General Data Protection Regulation; data subject rights.

Resumo

O artigo examina se e como os direitos dos titulares de dados, conforme o Regulamento Geral de Proteção de Dados (GDPR) europeu, podem ser exercidos dentro de sistemas de blockchain. Dadas as características técnicas das blockchains, a aplicação desses direitos parece ser desafiadora, ou até impossível, especialmente no que diz respeito ao direito ao apagamento, que é fundamentalmente comprometido pela imutabilidade da tecnologia blockchain. Este artigo apresenta as características técnicas das blockchains e explica as dificuldades associadas à aplicação dos direitos dos titulares de dados. Além disso, investiga quais atores envolvidos nas redes blockchain devem ser considerados controladores de dados, identificando, assim, as partes a quem os titulares de dados podem direcionar seus pedidos. Por fim, discute potenciais abordagens técnicas e organizacionais potenciais para resolver os conflitos identificados.

Palavras-chave: *Blockchain; proteção de dados; Regulamento Geral de Proteção de Dados; direitos dos titulares de dados.*

Introduction

Blockchain technology has gained significant attention since its first publication in 2008, when it was introduced in connection with the cryptocurrency

Bitcoin under the pseudonym Satoshi Nakamoto[2]. Since then, blockchain technology has expanded into a wide range of applications, particularly in the financial and insurance sectors, as well as in Industry 4.0. The defining technical characteristics of blockchain – namely, its decentralized structure and immutability – offer considerable advantages. By facilitating transparent and immutable transactions, blockchain ensures a high level of trust within the network. Additionally, its automation potential enhances business process efficiency and reduces costs (e.g., through smart contracts). However, the decentralized and immutable nature of blockchains raises questions about whether the legal requirements of the General Data Protection Regulation (GDPR) can be fulfilled, and whether blockchain technology can be operated in a legally compliant manner. In particular, enforcing data subject rights appears challenging due to the fundamental technical properties of blockchains.

This article explores whether and how data subject rights under GDPR can be enforced within blockchain networks. To this end, Section B. first provides an overview of blockchain's technical foundations and categorizes various technical and conceptual blockchain models. Section C. then analyzes the challenges and complexities of enforcing data subject rights, and finally, Section D discusses potential technical and organizational approaches to address these conflicts.

Technical Basics of Blockchain Technology

Before discussing the enforcement of data subjects' rights in the blockchain, a technical understanding of the technology is required. It should be noted that there is not only one single blockchain technology[3]. Rather, blockchains should be viewed as a class of technologies with different technical and conceptual characteristics[4]. These differences between blockchain systems must be taken into account when considering them from a legal perspective. To ensure this is successful, the technical basics will be explained below and the different variants of the blockchain systematized.

Basic structure and functionality of blockchains

A blockchain is a distributed database, or "distributed ledger", that operates on a peer-to-peer network[5]. Unlike centralized transaction systems, a blockchain network has no central components or control structures[6]. Data is stored and distributed within the network by its participants, or "nodes", which are interconnected with equal rights and responsibilities[7]. Each participant in the blockchain network replicates, validates, and stores a copy of the blockchain database, ensuring that everyone has access to the complete transaction history across the entire database[8].

Transactions involving asset transfers are executed within a blockchain network[9]. Each transaction contains the necessary information to facilitate the value transfer, such as the sender and recipient addresses, account balances, and the amount transferred in the case of

[2] Nakamoto, Bitcoin, 2008.

[3] EU Parliament, 2019, p. 1; BSI, Blockchain sicher gestalten, 2019, p. 11; Zentgraf, 2024, p. 39; Bitkom, Faktenpapier 2017, p. 3.

[4] EU Parliament, 2019, p. 1; see Peitz, 2020, p. 42.

[5] Bechtolf/Vogt, ZD 2018, p. 67; Justizministerkonferenz, Bericht 2019, p. 262; BMVI, 2019, p. 2.

[6] Zentgraf, 2024, p. 45; see BMVI, 2019, p. 3.

[7] Zentgraf, 2024, p. 45; Conference of Ministers of Justice, Report 2019, p. 264.

[8] Hein/Wellbrock/Hein, 2023, pp. 6, 7; Conference of Ministers of Justice, Report 2019, p. 264.

[9] See Sydow, in Sydow/Marsch, GDPR, BDSG, Introduction, para. 178.

monetary transactions[10]. The transaction data is then introduced into the blockchain network and consolidated into a block[11].

As peer-to-peer networks generally do not have a central authority that determines the correct status of the transaction history and checks the legitimacy of transactions, a consensus mechanism is required to verify completed transactions and for the network participants to agree on a specific transaction chronology[12]. Depending on the type of blockchain, different types of consensus mechanisms can be considered[13]. For public blockchain networks[14], a common consensus mechanism is the "Proof of Work", in which the network participants involved in the validation solve a cryptographic puzzle as "Proof of Work" and the first participant to find the solution receives a reward[15]. An alternative to the "Proof of Work" is the "Proof of Stake", in which the consensus is also realized by the network participants, but only a limited number of authorized participants carry out the validation of transactions and the formation of new blocks[16]. In private blockchain networks requiring authorization[17], however, validation takes place differently. Here, a central authority is selected by the operator of the blockchain network to monitor the network and the consensus mechanism[18]. In contrast to the "Proof of Stake", the central authority is known and has therefore been entrusted with the task of validation as a trustworthy entity[19].

The network participants involved in the validation process check the validity of the transaction data, combine valid transactions into blocks and send these into the blockchain network[20]. The other participants then check the data of the new block and accept it by adding it to their copy of the blockchain[21]. In this way, the transactions are verified and accepted throughout the network. This process is continuously repeated with new transactions so that new blocks are constantly created and the blockchain is growing[22].

The functionality of blockchain technology is also based on the use of hash functions[23]. Using hash functions, any data record can be converted into a hash value, i.e. a character string[24]. As hash functions are deterministic, the hash value can be used to check transaction data for changes, regardless of its type and size[25]. In the blockchain, hash functions are also used to link the blocks within the chain[26]. The hash values determined from transaction data act as a reference to the data of the previous and subsequent blocks[27]. This makes the entire history of transactions and the assignment to the respective participants completely traceable[28]. This characteristic of the blockchain means that data stored on the blockchain is practically unchangeable: any change to data would lead to a change in its hash value and thus to a change in the hash values of the

[10] Hein/Wellbrock/Hein, 2023, p. 9; Zentgraf, 2024, p. 58.

[11] Conference of Ministers of Justice, Report 2019, p. 266; Peitz, 2020, p. 41; Hein/Wellbrock/Hein, 2023, p. 9.

[12] Peitz, 2020, p. 42, 48.; Zentgraf, 2024, p. 74; Nakamoto, Bitcoin, 2008, p. 2.

[13] Zentgraf, 2024, p. 76.

[14] Definition and systematization of the different network variants in section B.II.

[15] Zentgraf, 2024, p. 77.; Conference of Ministers of Justice, Report, p. 269; Peitz, 2020 p. 50.

[16] Zentgraf, 2024, p. 80; Adam, 2022, p. 33.

[17] Definition and systematization of the different network variants in section B.II.

[18] Zentgraf, 2024, p. 82; BNetzA, 2021, p. 13; Janicki/Saive, ZD 2019, p. 255; EU Commission, 2019, p. 25.

[19] Zentgraf, 2024, p. 82.

[20] Peitz, 2020, p. 49; Martini/Weinzierl, NVwZ 2017, p. 1252.

[21] Peitz, 2020, p. 51; Nakamoto, Bitcoin, 2008, p. 3.

[22] Guggenberger, ZD, 2017, p. 49; Peitz, 2020, p. 52.

[23] Zentgraf, 2024, p. 61; Peitz, 2020, p. 18; Erbguth, MMR 2019, p. 654; Adam, 2022, p. 30.

[24] Peitz, 2020, p. 18; Gerth/Heim, 2022, p. 265; Adam, 2022, p. 30.

[25] Zentgraf, 2024, p. 62; Peitz, 2020, p. 19; Gerth/Heim, 2022, p. 265.

[26] Hein/Wellbrock/Hein, 2023, p. 11; Gerth/Heim, 2022, p. 185: Zentgraf, 2024, p. 64.

[27] Zentgraf, 2024, p. 63; Hein/Wellbrock/Hein, 2023, p. 11.

[28] Peitz, 2020, p. 40.

entire blockchain[29]. In order to include the change in the blockchain, all subsequent blocks in the blockchain would have to be revalidated, which is practically impossible due to the computing power required for this[30].

To process transactions on the blockchain, they are encrypted using asymmetric encryption[31]. On the one hand, this ensures that transactions are only decrypted by authorized network participants and protected against access by unauthorized persons[32]. On the other hand, asymmetric cryptography is used for the digital signing of transactions to identify the participants, thus ensuring that transactions have been legitimately initiated[33]. In asymmetric encryption, a key pair – consisting of a public and a private key – is used[34]. The public key is openly accessible and enable the transaction sender to encrypt the transaction[35]. The private key, on the other hand, is kept secret and is used by the owner (and transaction recipient) to decrypt and digitally sign transactions[36]. Transactions are assigned to a network participant via their user account, which is linked to the public key[37]. In this respect, the public key acts as a kind of account number for the network participant and is referred to as their "blockchain address"[38]. The private key, on the other hand, can be compared to a signature[39] of the transaction sender as well as a password[40]. Unlike a conventional password, the private key cannot be reset or replaced, meaning that it is not possible to restore the private key if it is lost[41]. In the event of loss, the user irrevocably loses access to transactions carried out[42].

Systematization of the blockchain variants

Blockchains have different technical and conceptual characteristics. On the one hand, blockchain systems can be divided into public and private blockchain systems according to the group of authorized users[43]. On the other hand, a further differentiation can be made based on the validation permission of the blockchain into permissionless and permissioned blockchains[44].

Public and private blockchains

The distinction between public and private blockchain networks is based on who is allowed to participate in the blockchain network[45].

If anyone can participate in the blockchain network, it is a public blockchain[46]. Public blockchains allow participants to feed data into the blockchain network without restriction and to view all transactions that are added to the blockchain[47]. To participate, it is sufficient for the

[29] Adam, 2022, p. 30; Peitz, 2020, p. 40.
[30] Peitz, 2020, p. 40.
[31] Peitz, 2020, p. 22; Zentgraf, 2024 p. 65.
[32] Zentgraf, 2024, p. 65.; Peitz, 2020, p. 22.
[33] Zentgraf, 2024, p. 65; Peitz, 2020, p. 22.
[34] Peitz, 2020, p. 22.; Hein/Wellbrock/Hein, 2023, p. 8; Petrlic/Sorge, Datenschutz, 2017, p. 15.
[35] See Peitz, 2020, p. 23.; Zentgraf, 2024, p. 70.
[36] Pohlmann, Cyber-Sicherheit, 2022, p. 543; Schrey/Thalhofer, NJW 2017, p. 1432.
[37] Peitz, 2020, p. 23.
[38] Hofert, ZD 2017, p. 163; Peitz, 2020, p. 23; Pohlmann, Cyber-Sicherheit, 2022, p. 543.
[39] Peitz, 2020, p. 24.
[40] Martini/Weinzierl, NVwZ 2017, p. 1252.
[41] Zentgraf, 2024, p. 72.
[42] Zentgraf, 2024, p. 72.
[43] Hein/Wellbrock/Hein, 2023, p. 12; Bitkom, Faktenpapier, 2017, p. 9; BMVI, 2019, p. 37.
[44] Zentgraf, 2024, p. 50.
[45] Zentgraf, 2024, p. 51; Bitkom, fact paper, 2017, p. 9; Adam, 2022, p. 21; Saive, CR 2018, p. 187.
[46] Zentgraf, 2024, p. 51; EU Parliament, 2019, p. 5; Isler, 2017, p. 4; Saive, CR 2018, p. 187.
[47] BSI, Blockchain sicher gestalten, 2019, p. 11. BMVI, 2019, p. 37.

participant to install the freely accessible blockchain software on their computer[48]. In this respect, the type of access can be compared to a website that is publicly accessible on the Internet[49]. The participants in the network do not know each other and trust the network because of the consensus model chosen[50]. In practice, cryptocurrencies such as Bitcoin and Ethereum are based on the concept of a public blockchain[51].

Unlike a public blockchain, the circle of participants in private blockchains is limited to a specific group of people[52]. A central authority determines access[53]. Unlike public blockchains, private blockchains focus on knowing the identity of the participants and ensuring the integrity of the database[54]. Practical applications include, for example, consortium projects of banks or insurance companies for more efficient business processing between the institutions involved in the project[55]. A practical example is a project launched in 2017 between Daimler and the Bank of Baden-Württemberg, which used a private blockchain was used for promissory note transactions[56].

Permissioned and permissionless blockchains

A further technical and conceptual differentiation of blockchains can be made based on the permission to participate in the validation process, i.e. to verify blocks and update the blockchain[57]. In this regard, a distinction is made between permissionless and permissioned blockchains[58]. If all participants are authorized to participate in the validation process, it is a permissionless blockchain[59]. Permissionless blockchains are particularly suitable for public blockchains[60]. Examples of permissionless blockchains are again the cryptocurrencies Bitcoin and Ethereum[61]. If the authorization to participate in the validation process is restricted, it is a permissioned blockchain[62]. In the case of permissioned blockchains, only a limited number of trusted participants are authorized to validate blocks[63], such as a central authority designated by the blockchain operator[64]. Permissioned blockchains are relevant in the financial and insurance sectors, for example[65].

Systematization matrix

The access and authorization variants shown can be combined with each other, depending on the area of application. In addition to the most open variant of the public, permissionless blockchain, public permissioned blockchains are also possible if the network is accessible to everyone, but only a limited group of participants is authorized to validate blocks[66]. In addition

[48] Peitz, 2020, p. 62; EU Parliament, 2019, p. 5; Conference of Justice Ministers, Report 2019, p. 264.

[49] Peitz, 2020, p. 62.

[50] Zentgraf, 2024, p. 51.

[51] Peitz, 2020, p. 62; Isler, 2017, p. 4; Conference of Ministers of Justice, Report, 2019, p. 263.

[52] Peitz, 2020, p. 63; BMVI, 2019, p. 37; Saive, CR 2018, p. 187.

[53] Peitz, 2020, p. 63; Conference of Ministers of Justice, Report, 2019, p. 263.

[54] Peitz, 2020, p. 63.

[55] Isler, 2017, p. 4; see Peitz, 2020, p. 63; see BSI, Blockchain sicher gestalten, 2019, p. 11.

[56] See press release from Landesbank Baden Württemberg dated 28/07/2017, available at: https://www.lbbw.de/artikelseite/pressemitteilung/daimler-und-lbbw-setzen-blockchain-bei-schuldschein-transaktion-ein_8zvetwhio_d.html.

[57] BSI, Blockchain sicher gestalten, 2019, p. 11; Zentgraf, 2024, p. 53; Peitz, 2020, p. 65.

[58] Adam, 2022, p. 21; Zentgraf, 2024, p. 53; BMVI, 2019, p. 37; Saive, CR 2018, p. 187.

[59] BSI, Blockchain sicher gestalten, 2019, p. 11; Isler, 2017, p. 5; Zentgraf, 2024, p. 54; BMVI, 2019, p. 37.

[60] Zentgraf, 2024, p. 54.

[61] Peitz, 2020, p. 66; Weizel/Eckert/Kristein/Jacumeit, 2017, p. 15.

[62] Peitz, 2020, p. 65; Bechtolf/Vogt, ZD 2018, p. 69.

[63] Isler, 2017, p. 5; BSI, Blockchain sicher gestalten, 2019, p. 11; BMVI, 2019, p. 37; Burgwinkel, 2016, p. 35.

[64] See section B.I.2.b.

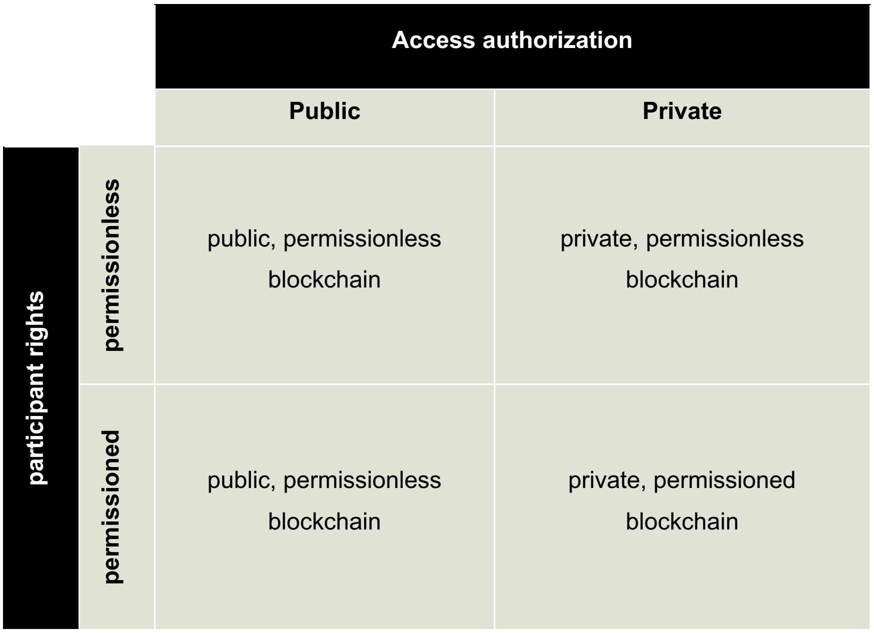
[65] Peitz, 2020, p. 67.

[66] Peitz, 2020, p. 67; Saive, CR 2018, p. 187; Adam, 2022, p. 22.

to the most restrictive variant of the private permissioned blockchain, a private, permissionless blockchain is also conceivable, provided that all authorized participants have validation rights[67]. In practice, the most common use cases are those of the public permissionless blockchain and the private permissioned blockchain[68]. As a result, the following systematization can be made.

Enforcement of Data Subject Rights In Blockchains

The rights of data subjects are regulated in Chapter 3 of the GDPR, whereby Art. 12 GDPR contains general regulations on the rights of data subjects, Art. 13 and 14 GDPR regulate the information obligations of the Controller and Art. 15 et seq. contain the individual rights of data subjects, such as the right of access in Art. 15 GDPR, the right to rectification in Art. 16 GDPR and the right to erasure and to be forgotten in Art. 17 GDPR.



		Access authorization	
		Public	Private
participant rights	permissionless	public, permissionless blockchain	private, permissionless blockchain
	permissioned	public, permissionless blockchain	private, permissioned blockchain

Figure 1 – Diagram relating public and private access authorization with the rights of the participant with and without permission. Source: Prepared by the author (2024).

In light of the technical characteristics of blockchains described above, it appears questionable whether and, if so, how data subjects can effectively enforce their data protection rights in blockchains. On the one hand, data subjects face the upstream problem of identifying a Controller against whom they can assert their data subject rights. On the other hand, the question arises as to how data subject rights can be implemented given the technical characteristics of blockchains. Based on the presentation and systematization of blockchain variants in section B., the following section first examines who is the Controller under data protection law and thus the addressee of data subject rights. It then examines the challenges involved in the technical implementation of data subject rights. The focus is on the rights to information, rectification

[67] Peitz, 2020, p. 68; Saive, CR 2018, p. 187.

[68] Peitz, 2020, p. 68.

and erasure, as these appear to be particularly affected by blockchain technology. Finally, further practical problems that can arise when asserting data subject rights are briefly discussed.

Identification of the Controller

If data subjects want to enforce their data protection rights, they need an addressee to whom they can assert their rights. According to Art. 12 GDPR, the addressee of the data subject rights is the Controller of the data processing. Determining the Controller is therefore important from the data subject's perspective in order to be able to enforce data protection rights. Nevertheless, determining the correct Controller for blockchains appears to be a challenge, as the processing of personal data is decentralized and involves a large number of different actors[69]. In the following, the role of the Controller under GDPR will first be defined and then, based on the systematization carried out in section B.II., it will be examined which of the actors involved in the blockchain are to be regarded as Controllers.

Concept of responsibility under GDPR

Under the GDPR, responsibility for data processing is allocated to a defined Controller as specified in Article 4 No. 7 GDPR. According to Art. 4 No. 7 GDPR, the Controller is any natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data[70]. In order to determine the Controller, a factual assessment must be made, taking into account all circumstances that justify the control[71]. If several actors jointly decide on the purposes and means of data processing, they are Joint Controllers in accordance with Art. 4 no. 7, Art. 26 para. 1 sentence 1 GDPR.

Controllership within blockchains

Due to the decentralized structure of blockchains and the large number of actors involved, it is not easy to identify a specific person or entity that has the sole power to decide on the purposes and means of data processing. The determination of the Controller must be assessed individually for each specific blockchain variant.

(a) Public blockchains (permissioned/permissionless)

In public blockchain networks, there is no instance that has centralized control options[72]. The circle of potential Controllers is large[73]. All actors involved can be considered: the developer of the blockchain software, the operator of the blockchain and the participants who carry out transactions in different roles, participate in the validation and creation of new blocks or merely store a copy of the blockchain as so-called "light nodes"[74].

Software developer and operator of the blockchain

The software developer, who initially influences the technical design of the blockchain, might be considered as the Controller under data protection law[75]. However, the software developer

[69] See Zentgraf, 2024, p. 177.

[70] Klabunde/Horváth in Ehmann/Selmayr, 2024, GDPR Art. 4 para. 39; Janicki/Saive, ZD 2019, p. 253.

[71] Klabunde/Horváth in Ehmann/Selmayr, 2024, GDPR Art. 4 para. 39; EDPB, Guidelines 7/2020, para. 21.

[72] Peitz, 2020, p. 209; Gerth/Heim, 2022, p. 197.

[73] Peitz, 2020, p. 209.

[74] Zentgraf, 2024, p. 188; Martini/Weinzierl, NVwZ 2017, p. 1253; Bitkom, fact paper, 2017, p. 28.

[75] Zentgraf, 2024, p. 191; Quiel, DuD 2018, p. 569; Erbguth/Fasching, ZD 2017, p. 564.

does not qualify as a Controller, as he relinquishes control over the purposes and means of data processing upon the blockchain's launch and the publication of its code[76]. At the time at which the software developer influences the design of the blockchain, no personal data is processed due to the lack of participant transactions[77]. Similarly, the responsibility of the operator of a blockchain is also excluded, insofar as it differs from the developer[78]. The operator only provides the application itself and also relinquishes control over the purposes and means of data processing when the blockchain goes live[79].

Network participants

The individual participants within the blockchain network can be considered as data Controllers under GDPR. The participants can perform different functions and act in different roles[80].

(a) Participants who carry out transactions

By carrying out transactions, participants feed personal data into the blockchain network. Some scholars, along with the *Bitkom*, argue against assigning the role of a Controller to these participants[81]. *Peitz*, for example, considers the actual influence on data processing to be minimal, as it is ultimately limited to providing technical input in the form of transaction data, without any control over subsequent data processing within the blockchain network[82]. *Gerth/Heim and Quiel*, reject Controllership too, arguing that no individual participant, nor any group of participants, has the authority to determine the purposes and means of data processing[83].

However, another segment of the literature, along the French CNIL qualifies participants who carry out transactions as data Controllers[84]. This view is supported by the argument that, by executing transactions, participants enable personal data (e.g. sender and recipient address, number of bitcoins transferred[85]) to be fed into the blockchain network and processed[86]. In the context of a transaction, participants also determine the specific purposes of the data processing, specifically the processing of the initiated transaction and their participation in the network[87]. This view is compelling because participants who initiate transactions control the entry of the resulting data into the network, its validation according to the established consensus mechanism, and its eventual inclusion in the blockchain. Without the execution of their transactions, the network would not process any personal data. In this sense, they indeed influence the purposes and means of processing.

(b) Participants who validate transactions

Some scholars and the CNIL reject the Controllership of the participants involved in the validation of transactions and block creation, arguing that their role is limited to validating blocks.

[76] Bitkom, fact paper, 2017, p. 28; Zentgraf, 2024, p. 191; Erbguth/Fasching, ZD 2017, p. 564.
[77] Zentgraf, 2024, p. 191.
[78] Zentgraf, 2024, p. 190; Martini/Weinzierl, NVwZ 2017, p. 1253; Bitkom, fact paper, 2017, p. 28.
[79] Zentgraf, 2024, p. 190; Martini/Weinzierl, NVwZ 2017, p. 1253; Bitkom, fact paper, 2017, p. 28.
[80] Zentgraf, 2024, p. 192.
[81] Gerth/Heim, 2022, p. 197; Quiel, DuD, 2018, p. 569; Bitkom, Faktenpaper 2017, p. 28.
[82] Peitz, 2020, p. 213.
[83] Gerth/Heim, 2022, p. 197; Quiel, DuD 2018, p. 569.
[84] Zentgraf, 2024, p. 196; CNIL, Blockchain, 2018, p. 1; Schrey/Thalhofer, NJW 2017, p. 1433.
[85] Erbguth/Fasching, ZD 2017, p. 564.
[86] Zentgraf, 2024, p. 196; CNIL, Blockchain, 2018, p. 1; Erbguth/Fasching, ZD 2017, p. 564.
[87] Zentgraf, 2024, p. 197; Martini/Weinzierl, NVwZ 2017, p. 1253; Gerth/Heim, 2022, p. 197.

They contend that these participants do not influence the content or purpose of transactions, and therefore have no impact on the processing of personal data[88]. Furthermore, they operate within the established consensus mechanism and execute it concerning the transaction data input, effectively acting as "servants of the overall system"[89]. In contrast, another segment of the literature classifies participants involved in validation as data Controllers, as they provide their computing resources for the validation of transactions and the creation of new blocks, thereby determining whether a transaction and the resulting personal data are validated[90].

The classification of the participants involved in validation as data Controllers is compelling. While it is true that these participants do not influence the initial execution of a transaction or its intended purpose, they play a crucial role within the network. Through the validation process, they determine whether the personal data entered is added to the blockchain as a new block, thereby becoming part of the transaction history. In the *Wirtschaftsakademie Schleswig-Holstein* case, the European Court of Justice ruled that enabling data processing is sufficient to establish a link to determination[91]. Since participants decide on the facilitation of processing – specifically, whether to validate the transaction data – they also determine the specific purposes of processing and the means, which include the blockchain network and their own computing resources.

(c) Participants who store the blockchain

Participants, who only store transactions and distribute them within the network without performing any other functions, act as nodes (often referred to as "Light Nodes")[92]. Their primary role is to provide server capacity and ensure the technical functionality and currency of the blockchain by storing and disseminating transactions[93]. According to one perspective in the literature, Light Nodes are not considered data Controllers because, although they process transaction data through storage and distribution, they lack decision-making power regarding the purposes and means of the transactions[94]. Conversely, another viewpoint contends that Light Nodes should be classified as Controllers since they distribute new data to other nodes within the network and can independently decide on the means of processing, such as the blockchain software and hardware used, as well as the purposes of processing, including which transactions they choose to distribute and store a copy of[95]. The latter perspective is more convincing. Light Nodes play a crucial role in processing transaction data alongside other network participants who initiate and validate transactions. By distributing transactions within the network and adding validated data blocks to their copy of the blockchain, they facilitate the updating of the blockchain. Like other participants, they therefore influence the "whether" of data processing and qualify as Controllers under GDPR.

Private blockchains (permissioned/permissionless)

In contrast to public blockchain variants, private blockchains feature a central authority that acts as an intermediary, determining access to the blockchain network and monitoring

[88] Martini/Weinzierl, NVwZ 2017, p. 1253; CNIL, Blockchain, 2018, p. 2; Zentgraf, 2024, p. 195; European Parliament, 2019, p. 46; Bitkom, Faktenpapier, 2017, p. 28; Janicki/Saive, ZD 2019, p. 253.

[89] Martini/Weinzierl, NVwZ 2017, p. 1253.

[90] Peitz, 2020, p. 227; Bechtolf/Vogt, ZD 2018, p. 69; Schrey/Thalhofer, NJW 2017, p. 1433.

[91] ECJ, Case C-210/16, para. 35, 38; see also Wagner, ZD 2018, p. 309.

[92] Zentgraf, 2024, p. 192; Krupar/Strassemeyer, DSRITB, 2018, p. 347.

[93] Zentgraf, 2024, p. 192.

[94] Zentgraf, 2024, p. 193; Gerth/Heim, 2022, p. 197; Krupar/Strassemeyer, DSRITB, 2018, p. 347.

[95] Peitz, 2020, p. 221; similarly: Martini/Weinzierl, NVzW 2017, p. 1253.

its activities[96]. Alongside the software developer, the operator of the blockchain, and the participants in their various roles, this central authority can also be regarded as a data Controller under GDPR[97].

Software developer

The role of the software developer in private blockchains should be dismissed for the same reasons as in public blockchains[98].

Participants

Similar to public blockchains, it is essential to distinguish between the individual functions of participants in private blockchains to ascertain their roles as Contrrollers under GDPR.

(a) Participants who carry out transactions

If participants have their own decision-making authority regarding transactions, they are considered data Controllers, similar to the situation in public blockchains[99]. For example, this would apply if a private blockchain were used for trading shares and fund units, allowing individual users to independently purchase shares. In such cases, the role of blockchain participants would be comparable to those in public[100]. However, the scenario where the control structure shifts from individual network participants to the operator of the blockchain network must be evaluated differently[101]. Participants in private networks may be compelled to accept the operator's conditions and carry out transactions based on its specified purposes[102]. In business models that utilize a private blockchain, there is typically a vested interest for the operator to maintain control over both participants and data processing (e.g., when a blockchain is managed by a banking consortium)[103]. If participants do not execute transactions in their own interest but rather in the interest of the operator, following its instructions and under a corresponding contract for data processing on behalf as stipulated in Article 28 GDPR, they act as Processors and therefore do not qualify as Controllers[104].

(b) Participants who validate transactions

In private blockchains, validation is typically performed by a central authority designated for this purpose[105]. This entity acts on behalf of and under the instructions of the operator of the blockchain network, qualifying as a processor if a data processing agreement has been established in accordance with Article 28 para. 3 GDPR[106]. As a result, there is no data protection responsibility attributed to this entity as a Controller.

[96] Peitz, 2020, p. 228; Bitkom, fact paper, 2017, p. 30; BMVI, 2019, p. 134.
[97] Zentgraf, 2024, p. 205; Gerth/Heim, 2022, p. 198.
[98] See section C.I.2.a.(1).
[99] Janicki/Saive, ZD 2019, p. 255.
[100] See section C.I.2.a.(2)(a).
[101] Peitz, 2020, p. 230.
[102] Zentgraf, 2024, p. 207.
[103] Peitz, 2020, p. 229; Saive, CR, 2018, p. 187.
[104] Martini/Weinzierl, 2017, p. 1254; BMVI, 2019, p. 134; Janicki/Saive, ZD 2019, p. 255.
[105] See section B.I.1.b.
[106] Janicki/Saive, ZD 2019, p. 256.

(c) Participants who store the blockchain

Participants who distribute and store transaction data without being subject to the instructions of the authority of the blockchain network are also to be qualified as data Controllers in private blockchains, applying the same reasoning as for public blockchains[107].

Operator of the blockchain

Whether the operator of a private blockchain qualifies as a Controller depends on the specific design of the blockchain network. If the operator of the private blockchain merely provides technical access and does not exercise any control over the purposes and means of the transactions conducted by participants, it is not considered a Controller[108]. Instead, it could act as a Processor, provided it has established a corresponding data processing agreement with the participants in accordance with Article 28 GDPR. In this scenario, an entity responsible for validation would serve as a sub-processor.

Conversely, the operator of the blockchain is deemed a data Controller if it not only determines access to the network but also maintains full control over the purposes for which transactions are conducted within the blockchain[109]. In such a constellation, the operator would issue instructions to network participants regarding transactions to be executed, and these participants would then act as processors.

Central authority

If the operator commissions a central authority to validate transactions, it is generally regarded as a Processor. The central authority may also be tasked by the initiator of the blockchain with additional responsibilities, such as deciding on the admission of participants to the blockchain network. Several roles are possible in this context. For example, the central authority could act as a Processor when determining participant admissions, provided it operates under the instructions of the operator and has established a data processing agreement in accordance with Article 28 GDPR. Additionally, the operator and the central authority may qualify as Joint Controllers under Article 26 GDPR if they jointly determine the purposes and means of data processing during the admission process.

Conclusion

In both public and private blockchains, the software developer can be excluded as a data Controller. While all participants in public blockchains are data Controllers under GDPR – carrying out, validating and distributing transactions and storing a copy of the blockchain – differences may arise in private blockchains depending on their design. In private blockchains, the central authority responsible for validating transactions typically acts as a processor rather than a Controller. Participants who execute transactions, distribute them, and store a copy of the blockchain are considered data Controllers in private blockchains if, similar to public blockchains, they operate independently of any instructions from the blockchain operator and conduct transactions for their own purposes. Conversely, the blockchain operator is classified as the Controller if it determines the purposes of the transactions and the participants execute them according to its instructions.

[107] See section C.I.1.2.a.(2)(c).

[108] See Janicki/Saive, ZD 2019, p. 255; Zentgraf, 2024, p. 206; Saive, DuD 2018, p. 765.

[109] Janicki/Saive, ZD 2019, p. 255; Martini/Weinzierl, NVwZ 2017, p. 1254; Gerth/Heim, 2022, p. 198.

II. Technical implementation of data subject rights

Having clarified to whom data subjects can assert their data protection rights, the technical challenges associated with implementing these rights will now be examined.

1. Right to information and copy (Art. 15 GDPR)

According to Art. 15 para. 1 GDPR, data subjects have the right to request information from the Controller regarding whether their personal data is being processed and, if so, which specific data is involved. In addition, the Controller is required to provide further information in accordance with Art. 15 para. 1 GDPR, such as the purpose of the processing and the recipients of the data. The right to information is supported by Art. 15 para. 3 GDPR, which entitles data subjects to request a copy of their processed personal data; only those who understand the extent to which their data is processed by the controller can effectively exercise their rights to rectification, erasure, and so on[110].

The use of a blockchain does not present any fundamental obstacles or unique challenges to the provision of information by the Controller[111]. Due to the transparent and seamless storage of all transactions on the blockchain, information about the processing of personal transaction data and its history should generally be accessible[112]. If the Controller is only able to provide encrypted data or hash values, the data subject can decrypt this information using their private key[113]. In principle, the other general information required under Art. 15 para. 1 lit. a), d), e), f) and h) GDPR should also be readily available[114].

2. Right to rectification and completion (Art. 16 GDPR)

According to Art. 16 GDPR, the data subject may request the rectification of inaccurate data or, if incomplete data is processed, the completion of that data. As described in section B.I.2.c., one of blockchain's core features is the immutability of transactions once they have been validated and added to the blockchain as part of a block. Technically, data on the blockchain can be altered[115]. However, any modification would require updating all subsequent hash values across the entire chain, necessitating the revalidation of each block[116]. Given the significant resources this would require, altering data on the blockchain is effectively impossible, particularly for transactions that occurred long ago[117].

The rectification of data on a blockchain can only be achieved by deleting incorrect data and then adding corrected data[118]. Since deletion is not feasible for the reasons outlined, the right to rectification fundamentally conflicts with blockchain's technical properties[119].

However, the situation differs for the right to complete data. Completion entails adding further information to existing data, which can be done through a supplementary declaration[120].

[110] Brink/Joos, ZD 2019, p. 483; Mester in Tager/Gabel, 2022, Art. 15 GDPR, para. 1.
[111] EU Parliament, 2019. p. 72; BMVI, 2019. p. 144; BSI, Blockchain sicher gestalten, 2019, p. 62.
[112] Gerth/Heim, 2022, p. 205; CNIL, Blockchain, 2018, p. 8; Zentgraf, 2024, 2024, p. 284.
[113] Zentgraf, 2024, p. 284.
[114] Zentgraf, 2024, p. 285.
[115] Zentgraf, 2024, p. 287; Krupar/Strassemeyer, DSRITB, 2018, p. 353.
[116] Zentgraf, 2024, p. 287; Peitz, 2020, p. 40.
[117] Gerth/Heim, 2022, p. 206; Peitz, 2020, p. 40.; Zentgraf, 2024, p. 287.
[118] Krupar/Strassemeyer, DSRITB, 2018, p. 353.
[119] EU Parliament, 2019. p. 72; Zentgraf, 2024, p. 285.
[120] *Kamann/Braun*, in Ehmann/Selmayr, 2024, GDPR Art. 16 para. 41; Gerth/Heim, 2022, p. 206.

Participants with write access to the blockchain – those able to initiate transactions – can thus add new transactions to supplement previously incomplete data[121]. It is irrelevant that the original incomplete data and the supplementary information are not combined in the same block[122].

3. Right to erasure, "right to be forgotten" (Art. 17 GDPR)

The right to erasure (the "right to be forgotten") under Art. 17 GDPR requires the Controller to erase personal data in the cases listed in paragraph 1 lit. a to f. Art. 17 GDPR itself does not provide a legal definition of "erasure"[123]. However, guidance can be drawn from the definition in Section 3 para. 4 no. 5 Federal Data Protection Act (old version), which described erasure as "making stored personal data unrecognizable"[124]. Data is considered erased when it is effectively impossible to retrieve or recognize the information previously contained in the data, with no one able to access this information without disproportionate effort[125]. Notably, the obligation to erase data does not apply universally; Art. 17, para. 3 GDPR specifies several exceptions in which the Controller is not required to erase the data.

Similar to the right to rectification, the fundamental technical structure of blockchain also conflicts with the right to erasure[126]. Due to the continuous and irreversible recording of transactions on the blockchain, a tension arises between "not being able to forget" and "the requirement to forget"[127]. Implementation is further complicated by the fact that all network participants store at least a portion, if not a complete copy, of the blockchain on their devices . Each of these copies would also need to be erased. Additionally, if a participant no longer engages with the network, they may still retain an outdated version of the blockchain. In public blockchains, the decentralized nature means participants are generally anonymous and cannot be contacted for deletion requests. Both the CNIL[129] and the European Parliament[130] have acknowledged that implementing the right to erasure on the blockchain is either technically impossible or highly challenging.

Conclusion

In conclusion, the right to information and access to a copy, as well as the right to data completion, are at least technically feasible in principle. However, the right to rectification and the right to erasure present conflicts with the core technical features of blockchain, specifically the immutability of stored data.

III. Contacting the Controller

In addition to the challenges of identifying a Controller and and technically implementing data subject rights, there is also the practical challenge of establishing contact with the identified Controller to assert these rights. In private blockchains, where the operator and/or a central authority may qualify as the Controller, these entities are generally positioned to fulfill data subject

[121] Zentgraf, 2024, p. 287.
[122] Zentgraf, 2024, p. 287; Krupar/Strassemeyer, DSRITB, 2018, p. 353.
[123] *Herbst* in Kühling/Buchner, 2024, GDPR Art. 17 para. 37; European Parliament, 2019, p. 72.
[124] *Herbst* in Kühling/Buchner, 2024, GDPR Art. 17 para. 37.
[125] *Herbst* in Kühling/Buchner, 2024, GDPR Art. 17 para. 37.
[126] BSI, Blockchain sicher gestalten, 2019, p. 63; Peitz, 2020, p. 143. Bechtolf/Vogt, ZD 2018, p. 69.
[127] Martini/Weinzierl, NVwZ 2017, p. 1251.
[128] Gerth/Heim, 2022, p. 207.
[129] CNIL, Blockchain, 2018, p. 9.
[130] European Parliament, 2019, p. II.

rights directly. They can also facilitate contact by providing accessible contact information, such as a dedicated channel on a website, ensuring that data subjects can readily reach them[131].

In contrast, contacting a Controller in practice may be difficult, if not impossible, when network participants are designated as Controllers, particularly in the context of public blockchains[132]. On the one hand, the participants in a public blockchain and also often in private blockchains remain anonymous[133]; on the other hand, these participants frequently change as individuals join and leave the network[134]. Even if a participant could be identified as the Controller, particularly private individuals – who are often not legally trained – would likely struggle to navigate the complexities of fulfilling data subject rights in a legally compliant manner[135].

IV. Conclusion

Data subjects face three main challenges in enforcing their rights. First, they must identify a Controller under GDPR among the many actors involved, a task complicated by the various types of blockchains and the diverse roles of these actors. Second, the possibilities for the technical implementation of data subject rights quickly reach their limits. While the rights to information and completion are technically feasible in principle, the implementation of the rights to rectification and erasure is hindered by the immutability of the blockchain. Additionally, in the case of public blockchains, data subjects often lack any information about the Controller, making it unclear how they can even initiate contact.

These obstacles raise serious concerns about the protection of data subjects rights and freedoms and question whether blockchain networks can be operated lawfully under the GDPR. Furthermore, the inability to fully fulfill data subject rights exposes data Controllers to the risk of liability for damages to data subjects (as outlined in Art. 82 GDPR and general national regulations) or sanctions from supervisory authorities, such as fines under Art. 83 para. 5 lit. b) GDPR.

Solution Approaches

In order for blockchain technology to be operated in a legally compliant manner within the scope of the GDPR, the conflicts described must be resolved. Some technical, and organizational solution approaches are presented and evaluated below.

I. Technical solution approaches

Numerous technical approaches exist to partially resolve the fundamental conflict between the technical characteristics of blockchain technology and the implementation of data subject rights.

1. Zero knowledge proof procedure

One potential solution involves preemptively excluding the applicability of the GDPR by eliminating personal references. This can be achieved through the use of a so-called zero-knowledge

[131] Zentgraf, 2024, p. 283.
[132] Peitz, 2020, p. 235; Zentgraf, 2024, p. 282.
[133] Peitz, 2020, p. 58.
[134] Peitz, 2020, p. 235.
[135] Peitz, 2020, p. 235; see Quiel, DuD, 2018, p. 570.

proof method[136]. In this approach, transaction data is stored in a manner that allows the execution of a transaction to be recorded on the blockchain while ensuring that the identity of the participant remains concealed[137]. Participants in the blockchain network can verify the mathematical correctness of transactions without being privy to the specific details of those transactions[138].

2. Off-chain data storage

Another approach involves off-chain data storage[139], where data generated during transactions is not stored on the blockchain itself but rather kept separately outside of it[140]. In this method, the externally stored data is converted into a hash value, and only this hash is recorded on the blockchain[141]. Since only anonymous data is stored on the blockchain in this manner, the GDPR's material scope would not apply due to the absence of personal data processing. However, the GDPR would still govern the personal data stored externally. Fortunately, the rights to erasure and rectification would be easily achievable with respect to this off-chain data[142].

3. Redactable blockchain

Another technical solution is the use of so-called redactable blockchains[143], which are designed to be inherently modifiable[144]. The linking of individual blocks in this type of blockchain relies on Chameleon hash functions, which enable the generation of the same hash value through a "back door" despite alterations to the input data. This functionality allows changes to be made to the blockchain without disrupting its integrity[145]. As a result, redactable blockchains facilitate compliance with the rights to erasure and rectification[146].

4. Pruning

It is also feasible to technologically modify the blockchain in such a way that the hash trees created during blockchain updates can be pruned. This would allow for the deletion of personal data from older blocks that are no longer necessary. A block that is no longer essential for validating a new block can be discarded because the output of the subsequent block has itself become the new starting point for additional transactions.

5. Deletion of the public key assignment data

In private blockchain networks, it is possible to delete the data that associates a public key with its respective user, which is managed by the operator or the central authority[147]. Once this data is removed, the individual can no longer be identified, effectively leading to subsequent anonymization[148]. However, there is ongoing debate about whether this form of anonymization

[136] Martini/Weinzierl, NVwZ 2017, p. 1256; Gerth/Heim, 2022, p. 210; Adam, 2022, p. 42.
[137] Martini/Weinzierl, NVwZ 2017, p. 1256; Gerth/Heim 2022, p. 210; BMVI, 2019, p. 139.
[138] Gerth/Heim, 2022, p. 210; Zentgraf, 2024, p. 332.
[139] BMVI 2019, P. 172.
[140] BMVI 2019, p. 172; Zentgraf, 2024, p. 331
[141] Zentgraf, 2024, p: 332.
[142] BMVI 2019, p. 144; Zentgraf, 2024, p. 332; BNetzA, 2021, p. 22.
[143] BMVI, 2019, p. 146; Gerth/Heim, 2022, p. 183, 208; Conference of Ministers of Justice, Report 2019, p. 270.
[144] Conference of Ministers of Justice, Report, 2019, p. 270; Saive, DuD 2018, p. 766.
[145] Gerth/Heim 2022, p. 208; NRW, 2019, p. 270; Saive, DuD 2018, p. 766; Zentgraf, 2024, p. 329.
[146] Gerth/Heim, 2022, p. 209; Saive, DuD 2018, p. 766; Hein/Wellbrock/Hein, 2023, p. 40.
[147] Martini/Weinzierl, NVwZ 2017, p. 1256; Zentgraf, 2024, p. 337.
[148] Martini/Weinzierl, NVwZ 2017, p. 1256; Zentgraf, 2024, p. 337.

constitutes erasure as defined by Art. 17 GDPR[149]. Depending on whether one equates anonymization with erasure, the right to erasure could either be satisfied, or the applicability of the GDPR could be negated, thereby exempting the obligation to fulfill the right to erasure entirely.

6. Discussion of approaches

The zero-knowledge proof method and off-chain data storage strategies aim to exclude the application of the GDPR to data processed within the blockchain. Both approaches effectively eliminate conflicts with data subject rights. However, they do not address the technical challenge of erasure for blockchains that are not designed and operated from the outset to avoid storing personal data on-chain. These methods can only offer solutions for blockchains that do not disclose transaction details in terms of their purpose. Such an approach would contradict the fundamental principle of a traditional blockchain, where the complete transaction history must remain transparently accessible to all participants. Consequently, the zero-knowledge proof and off-chain data storage techniques can only provide partial solutions.

The redactable blockchain facilitates the complete fulfillment of the rights to rectification and erasure by addressing the issue of immutability. However, this technical approach diverges significantly from the original concept of blockchain. Once the blockchain loses its characteristic immutability, it essentially becomes a "normal" database, allowing its contents to be modified at will. This shift undermines the inherent trust in the unchangeable and fully documented transaction history. Consequently, the redactable blockchain does not effectively resolve the core issue.

While pruning hash trees can enable the right to erasure for transactions that are no longer necessary for updating the blockchain, this approach is contingent upon the irrelevance of those transactions. Therefore, deletion is not feasible when the transactions of the data subject remain pertinent. As a result, pruning offers only a limited technical solution.

If anonymization of data is considered equivalent to erasure under Art. 17 GDPR, then the right to erasure can be satisfied by deleting the assignment data associated with the public key in private blockchains. Conversely, if anonymization is not equated with erasure, the applicability of the GDPR may be excluded, meaning that the right to erasure cannot be fulfilled concerning the anonymized data. Therefore, deleting the allocation data can be a viable solution for private blockchains. However, it is important to note that indirect identification of the data subject may still be possible under certain circumstances, even after the allocation data has been deleted. For example, if multiple transactions are conducted using the same public key, a single transaction may still be linked to an individual by comparing it with other transactions or utilizing big data techniques[150]. This raises the likelihood of re-identification, especially in light of advancing technologies[151]. In such cases, only pseudonymization of the data can be assumed.

In conclusion, the technical approaches discussed provide at least partial solutions to the challenges posed by data protection rights in blockchain environments. By deleting the assignment data of the public key, data deletion can be effectively achieved in private blockchains. However, the other approaches do not offer a comprehensive solution. Some methods aim to eliminate the personal reference, thereby circumventing the applicability of the GDPR, which compromises

[149] For example, Stürmer, ZD 2020, p. 629, BNetzA, 2021, p. 22; in contrast, Roßnagel, ZD 2021, p. 192, in favor of equating anonymization with deletion.
[150] Martini/Weinzierl, NVwZ 2017, p. 1253.
[151] Peitz, 2020, p. 126.

the blockchain's inherent advantage of providing transparent documentation of the transaction history. Conversely, other approaches propose altering the fundamental technical concept of the blockchain to such an extent that it risks losing its key benefits.

II. Organizational solution for contacting the person responsible

As outlined in section C.III., data subjects may find it challenging, if not impossible, to contact responsible network participants in both public and private blockchain networks[152]. One potential solution to this issue is to facilitate indirect contact. Engaging with responsible parties through public or private forums, social media, or other online platforms could be effective in obtaining contact details[153]. Many public blockchain projects boast active communities that regularly exchange information online[154]. In the context of private blockchains, it could be beneficial to establish the provision of contact information as a prerequisite for network admission. However, if these options are unavailable, there will be no feasible means to reach the responsible party, rendering the enforcement of data subject rights impossible. Given the large number of participants, many of whom may prefer to remain anonymous, this scenario is likely to occur frequently.

Summary and Overall Result

An examination of blockchain technology reveals considerable advantages due to its decentralized structure, immutability, and transparency. These technical features foster trust, ensure data security, and prevent manipulation, making blockchain valuable for numerous applications. However, as outlined in Section C. these same characteristics conflict with the enforceability of data subject rights under GDPR.

Several approaches exist to address this conflict. As discussed in Section D.I., there are technical solutions that can partially resolve the challenges of enforcing the rights to rectification and erasure. This is particularly relevant for data deletion in private blockchain networks, which can be achieved by removing the assignment data associated with the public key. Conversely, other technical solutions fail to fully address the issues surrounding the fulfillment of the rights to rectification and erasure without diverging from the fundamental principles and technical concepts of blockchain, thereby undermining some of its inherent advantages.

Section D. II. indicates that affected individuals might only be able to contact responsible blockchain participants through public forums or social media platforms, contingent upon those participants voluntarily disclosing their identity and contact details. In the case of private blockchains, participants could be contractually obligated to provide such information. However, this solution is often impractical, especially for public blockchains, rendering the assertion of data subject rights against responsible blockchain participants challenging.

To resolve these issues, legislative action is ultimately required to establish legal frameworks that facilitate the compliant and secure use of blockchain technology without altering or compromising its beneficial core principles.

Consequently, the research question can be answered by stating that the enforcement of data subject rights within blockchain technology is currently only partially achievable. Nevertheless,

[152] Zentgraf, 2024, p. 282.
[153] Zentgraf, 2024, p. 283.
[154] Zentgraf, 2024, p. 283.

various technical and organizational approaches are available to address the identified conflicts, either now or in the future. It is also worth noting that ongoing technological advancements may yield suitable solutions to fully uphold data subject rights under GDPR within the blockchain context.

Ultimately, whether the technical strengths of public blockchain networks can be effectively harnessed and further developed within the European Union and the European Economic Area, or whether data protection will become a "brake on innovation," hinges on resolving the conflict between data subject rights and the technical properties of blockchain.

Refrences

Adam, K. *Blockchain-Technologie für Unternehmensprozesse* – Sinnvolle Anwendung der neuen Technologie in Unternehmen. 2nd ed. Wiesbaden: Springer, 2022.

Bechtolf, H.; Niklas, V. O. G. T. *Datenschutz in der Blockchain – Eine Frage der Technik*. Zeitschrift für Datenschutz, No. 2. Munich: C.H. Beck, 2018. pp. 66-71.

Bitkom, E. V. *Blockchain und Datenschutz*. Fact Paper, 2017. Available from: https://www.bitkom.org/sites/default/files/file/import/180502-Faktenpapier-Blockchain-und-Datenschutz.pdf. Cited: 2024 Sep 10.

Brink, S.; Daniel, J. O. O. S. *Reichweite und Grenzen des Auskunftsanspruchs und des Rechts auf Kopie, Tatbestandlicher Umfang und Einschränkungen des Art. 15 DSGVO*. Zeitschrift für Datenschutz, No. 11. Munich: C.H. Beck, 2019, pp. 483-488.

Burgwinkel, D. *Blockchain Technology, Einführung für Business- und IT Manager*. Berlin: De Gruyter, 2016.

Commission Nationale Informatique & Libertés (CNIL). *Blockchain – Solutions for a responsible use of the blockchain in the context of personal data*. 2018. Available from: https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data. Cited: 2024 Sep 10.

Conference of The Independent Federal and State Data Protection Authorities (DSK). *Paper No. 6 - Auskunftsrecht der betroffenen Person, Art. 15 DSGVO*. 2018. Available from: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_6.pdf. Cited: 2024 Sep 10.

Eckert, K.-P. *et al. Mythos Blockchain*: Herausforderungen für den öffentlichen Sektor, Kompetenzzentrum Öffentliche IT. Competence Center Public IT, Fraunhofer Institute for Open Communication Systems FOKUS, 2017.

Ehmann, E.; Selmayr, M. *Beck'sche Kurz-Kommentare DS-GVO*. 3rd ed. Munich: Beck, 2024.

Erbguth, J.; Fasching, J. *Wer ist Verantwortlicher einer Bitcoin-Transaktion?* Anwendbarkeit der DSGVO auf die Bitcoin-Blockchain. Zeitschrift für Datenschutz, No. 12. Munich: Beck, 2017. p. 560-565.

Erbguth, J. *Datenschutzkonforme Verwendung von Hashwerten auf Blockchains* – Wann sind kryptografische Hashwerte von personenbezogenen Daten selbst wieder personenbezogene Daten? Zeitschrift für IT-Recht und Recht der Digitalisierung, No. 10. Munich: Beck, 2019. p. 654-660.

European Commission. *Blockchain Now And Tomorrow*: Assessing Multidimensional Impacts of Distributed Ledger Technologies. EU Science Hub, 2019. Available from: https://publications.jrc.ec.europa.eu/repository/handle/JRC117255. Cited: 2024 Sep 10.

European Data Protection Board (EDPB). *Guidelines 07/2020 on the Terms "Controller" and "Processor" in the GDPR*. Version 2.0. 2020. Available from: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_de. Cited: 2024 Sep 10.

European Parliament. *Blockchain and the General Data Protection Regulation* - Can Distributed Ledgers Be Squared with European Data Protection Law?. 2019. Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. Cited: 2024 Sep 10.

Federal Ministry Of Transport And Digital Infrastructure (BMVI). *Chancen und Herausforderungen von DLP (Blockchain) in Mobilität und Logistik*. Berlin, 2019. Available from: https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/1106/wi-1106.pdf. Cited: 2024 Sep 10.

Federal Network Agency. *Die Blockchain-Technologie – Grundlagen, Potenziale und Herausforderungen*. 2021. Available from: https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Technologien/Blockchain/Links_Dokumente/einfuehrung_bc.pdf?__blob=publicationFile&v=1. Cited: 2024 Sep 10.

Federal Office For Information Security (BSI). *Blockchain sicher gestalten - Konzepte, Anforderungen, Bewertungen*. Bonn, 2019. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf%3F__blob%3DpublicationFile%26v%3D5. Cited: 2024 Sep 10.

Gerth, S.; Home, L. *Entrepreneurship der Zukunft - Digitale Technologien und der Wandel von Geschäftsmodellen*. Wiesbaden: Springer, 2022.

Gola, P.; Heckmann, D. *General Data Protection Regulation Federal Data Protection Act Commentary*. 3rd ed. Munich: C.H. Beck, 2022.

Guggenberger, N. *Datenschutz durch Blockchain – eine große Herausforderung*. Zeitschrift für Datenschutz, No. 2. Munich: C.H. Beck, 2017. p. 49-50.

Hein, C.; Hein, C.; Wellbrock, W. *Rechtliche Herausforderungen von Blockchain-Anwendungen – Straf-, Datenschutz- und Zivilrecht*. 2nd ed. Wiesbaden: Springer, 2023.

Hofert, E. *Blockchain-Profiling, Verarbeitung von Blockchain-Daten innerhalb und außerhalb der Netzwerke*. Zeitschrift für Datenschutz, No. 4. Munich: C.H. Beck, 2017. p. 161-166.

Isler, M. *Datenschutz auf der Blockchain*. Editions Weblaw Jusletter, 2017.

Janicki, T.; Saive, D. *Privacy by Design in Blockchain-Netzwerken – Verantwortlichkeit und datenschutzkonforme Ausgestaltung von Blockchain*. Zeitschrift für Datenschutz No. 6. Munich: C.H. Beck, 2019. p. 251-256.

Krupar, F.; Strassemayer, L. *Datenschutz auf der Blockchain – die Innovationsfreundlichkeit der DSGVO*. Proceedings of the Autumn Academy, 2018. p. 343-359.

Kühling, J.; Buchner, B. *Gen Datenschutz-Grundverordnung / BDSG Kommentar*. 4th ed. Munich: C.H. Beck, 2024.

Martini, M.; Weinzierl, Q. *Die Blockchain-Technologie und das Recht auf Vergessenwerden*. Neue Zeitschrift für Verwaltungsrecht, No. 17. Munich: C.H. Beck, 2017. p. 1251-1259.

Ministry of Justice of The State of NRW. *Arbeitsgruppe „Digitaler Neustart" der Konferenz der Justizministerinnen und Justizminister der Länder*. Report of April 15 2019 – Robotic Law, Blockchain, Leistungsschutz an Daten. Available from: https://www.justiz.nrw/JM/justizpol_themen/digitaler_neustart/zt_fortsetzung_arbeitsgruppe_teil_2/2019-04-15-erichte_Apr_19_Okt_18_Druckfassung.pdf. Cited: 2024 Sep 10.

Nakamoto, S. *Bitcoin*: A Peer-to-Peer Electronic Cash System, 2008. Available from: https://bitcoin.org/bitcoin.pdf. Cited: 2024 Sep 10.

Peitz, C. *Datenschutzrechtliche Verantwortlichkeiten in Blockchain-Systemen*. Wiesbaden: Springer, 2020.

Petrlic, R.; Sorge, C. *Data Protection*: Introduction to Technical Data Protection, Data Protection Law, and Applied Cryptography. Wiesbaden: Springer, 2017.

Pohlmann, N. *Cyber-Sicherheit, Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*. 2nd ed. Wiesbaden: Springer, 2022.

Quiel, P. *Blockchain-Technologie im Fokus von Art. 8 GRC und DSGVO*. Datenschutz und Datensicherheit No. 9. Wiesbaden: Springer, 2018. p. 566-573.

Rossnagel, A. *Datenlöschung und Anonymisierung – Verhältnis der beiden Datenschutzinstrumente nach DSGVO*. Zeitschrift für Datenschutz, No. 4 Munich: C.H. Beck, 2021. p. 188-192.

Saive, D. *Haftungsprivilegierung von Blockchain-Dienstleistern gem. §§ 7 ff. TMG, Computer und Recht*. Computer und Recht, No. 3. Cologne: Otto Schmidt, 2018. p. 186-193.

Saive, D. *Rückabwicklung von Blockchain-Transaktionen*, Datenschutz und Datensicherheit No. 12. Wiesbaden: Springer, 2018. p. 764-767

Schrey, J.; Thalhofer, T. *Rechtliche Aspekte der Blockchain*. Neue Juristische Wochenschrift, No. 20. Munich: C.H. Beck, 2017. p. 1431-1436.

Stürmer, V. *Löschen durch Anonymisieren?* Mögliche Erfüllung der Löschpflicht nach Art. 17 DSGVO. Zeitschrift für Datenschutz, No. 12. Munich: C.H. Beck, 2020. p. 626–631.

Sydow, G.; Marsch, N. *Nomos Kommentar DSGVO BDSG Handkommentar*. 3rd. ed. Baden-Baden: Nomos, 2022.

Taeger, J.; Gabel, D. *Kommentar DSGVO – BDSG – TTDSG*. 4th. ed. Frankfurt am Main: dtv, 2022.

Wagner, B. *Disruption der Verantwortlichkeit – Private Nutzer als datenschutzrechtliche Verantwortliche im Internet of Things*. Zeitschrift für Datenschutz No. 7. Munich: C.H. Beck, 2018. p. 307–312.

Weiss, A. *Zivilrechtliche Grundlagenprobleme von Blockchain und Kryptowährungen*. Juristische Schulung, No. 11. Munich: C.H. Beck, 2019. p. 1050–1057.

Wolff, H. A.; Brink, S.; Antje, V. UNGERN-STERNBERG. *BeckOK Datenschutzrecht DS-GVO, DA, DGA, BDSG*. Datenschutz und Datennutzung. 48th. ed. Munich: C. H. Beck, 2024.

Zentgraf, Cl. K. J. *Blockchain im Spannungsfeld des europäischen Datenschutzrechts*. Studien zum Datenschutz. Baden-Baden: Nomos, 2024.