Towards GDPR Enforcing Blockchain Systems

Hauke Precht
Carl von Ossietzky Universität Oldenburg, Deutschland

Jorge Marx Gómez
Carl von Ossietzky Universität Oldenburg, Deutschland

Towards GDPR Enforcing Blockchain Systems

Hauke Precht[1], Jorge Marx Gómez[1]

[1] Carl von Ossietzky University of Oldenburg, Business Information Systems / VLBA, Oldenburg, Germany
{hauke.precht, jorge.marx.gomez}@uol.com

Abstract. This paper gives an overview of current research areas considering GDPR and blockchain. It is shown that GDPR is often seen as a problem, limiting blockchain use cases. However, approaches towards more data protection for the data subjects based on blockchain technology emerge. In this paper, we evaluate a first step towards a GDPR enforcing blockchain by using a combination of smart contracts within Hyperledger Fabric, evaluating if a *joint controllership agreement* is in place. Such agreement is required for joint controller to process personal data. Based on this rather simple use case evaluation, it is discussed that a combination of the different research areas around GDPR and blockchain should be further evaluated and combined, aiming to GDPR enforcing blockchain systems.

Keywords: *blockchain, GDPR, joint controllership agreement*

1 Introduction – GDPR and Blockchain

As blockchain gains more and more popularity and new application domains are included, the legal issues of blockchain are analyzed more often. Even though a variety of blockchains exist, they are typically classified in public, private, permissioned and permissionless blockchains [1]. Independent of this classification, they all build around the feature of the immutability of data. This is due to the fact, that the actual data structure "blockchain" is built as an ordered list of blocks, which contain transactions, chained via the hash representation of the previous block [1]. By combining this specific data structure with computational constraint and incentivizing block creation, a tamper-resistant and revisioning resistant decentralized system is built [1], which is also often referred to as blockchain. As the most used blockchain systems, Bitcoin, Ethereum and Hyperledger Fabric [2] all share the same described approach, they are all subject to the immutability feature. For the rest of the paper, when we speak about blockchains in general, we especially mean those blockchain systems which follow the described immutability feature by using a similar data structure. This immutability of data is of especially high interest in legal analysis as this can lead to violations of the General Data Protection Regulation (GDPR) rules when personal data is processed (e.g., the right of erasure cannot be fulfilled).

16th International Conference on Wirtschaftsinformatik,
March 2021, Essen, Germany

The most used approach to avoid possible violations is to store no personal data on the blockchain as done for example in [3]. However, in open systems like Bitcoin or Ethereum it is up to the user what they store, so violations are still possible. To avoid on-chain storage but still maintaining decentralized storage, approaches around the InterPlanetary File System (IPFS), which is a distributed file system on a peer-to-peer basis [4], emerged. Note, that even though decentralized off-chain storage could be used to store private data, it still falls under the GDPR, meaning a decentralized deletion of data must be possible. Note, that the idea to store private data in an encrypted way, especially on public blockchain with accessibility and readability for everyone is not considered to be GDPR compliant, as pointed out by Fridgen et. al. in their report for the German Federal Ministry of Transport and Digital Infrastructure [5, p. 137]. The authors argue, that as the encrypted data is stored *ad infinitum* on a public blockchain, the used encryption algorithm can be broken in the future leading to a state where the data can be considered publicly available, then violating the GDPR rules [5, p. 137]. But in the past few years, approaches were evaluated towards redactable blockchains, which aim to enable the modification of already accepted blocks [6–10]. This way, a possible modification or even erasure of data in a blockchain should be made possible to comply with the GDPR. But there also exist approaches, in which blockchain is considered as an enabler towards data sovereignty of the data subject. For example, blockchain technology is used to empower the data subject to manage its personal data via a blockchain-based personal data management platform [11, 12].

However, the GDPR does not only state the rights of data subjects, which can be challenging to fulfill in blockchain systems but also guidelines, targeting companies that process personal data. For example, in case personal data is processed by multiple controllers, Art. 26 GDPR must be considered [13], requiring a *joint controllership agreement (JCA)* between these controllers. In such a JCA, the controllers must define the internal relationship, stating whom of them are responsible to fulfill the different duties based on the GDPR. For example, it must be stated which controller(s) must fulfil the data subjects right of access as stated in Art. 15 GDPR. Considering blockchains in general, independent of access scope, i.e. private or public, all participants who operate a node take part in data processing and in case of processing personal data, GDPR must be considered [14]. Due to the high number of participants and anonymity in public blockchains, however, it is difficult to identify the actual controllers within such public blockchain networks. But in private blockchains, with limited and known participants, the controllers can be identified as well as the joint controllership [14] meaning a JCA can and must be implemented. Therefore, we will focus in the following of this paper on private and permissioned blockchain systems. In case no JCA is agreed on, every controller must provide the ability to fulfil possible requests from the data subjects as well as general duties based on the GDPR. Ignoring these duties and not creating a JCA high fines must be paid. Nevertheless, often there is no explicit JCA defined [15], but data is still processed in the blockchain system by smart contracts. In this paper, the authors evaluate a proposal consisting of a combination of smart contracts, enforcing a JCA to be in place before any data processing can be executed, therefore preventing legal uncertainty. Moreover, it is

discussed to evaluate possibilities to include such feature, and GDPR enforcing features in general, directly in (private and permissioned) blockchain systems. This could lead to further legal certainty and supporting the privacy by design approach as stated in Art. 25 GDPR. The paper is structured as follows: First, an overview of related work is given. Next, a prototypical implementation for a JCA smart contract combination within a private blockchain (Hyperledger Fabric) is given. This paper concludes with a short discussion towards GDPR enforcing blockchain systems.

2 Related Work

To ensure GDPR compliant implementation, different approaches can be identified. Wirth and Kolain presented in their paper a privacy by blockchain design, taking a step towards incorporating the privacy by design approach mentioned in GDPR, stating an interdisciplinary approach [16]. That an interdisciplinary approach is required to ensure legally compliant code, especially for smart contracts and blockchain systems, is also explained by Precht and Saive, who evaluate the integration of legal specialists into the scrum process [17]. The term smart contract was already coined by Szabos in 1979 [18]. In conjunction with blockchain, a new hype around smart contracts started. In general, a smart contract contains contractual rules as software code which is stored and executed on a blockchain [19]. To the best of the authors' knowledge, only two approaches explicitly dealing with the digitization of a JCA or related contract called data processing contract (DPC) with smart contracts. In [20] the authors propose a new specification of an intelligible contract, as a “gap between traditional contracts and digital contracts towards the goal of making them intelligible and legal valid.”[20]. They implemented a data processing agreement based on their newly created approach leading to a complex system [20]. In [13] the authors propose a different approach towards a digitized JCA. They evaluate, from a legal and technical perspective, the possibility to store the JCA on a private blockchain while also creating a smart contract around it, allowing parties to initiate, accept or to propose changes to a JCA. As the handling of the JCA is done on-chain as well, the whole development and creation phase of the JCA is transparent to all parties at every given time. Therefore, it can be said that this focus is towards the handling and tracking of the JCA process itself as an asset on the blockchain between parties, while [20] focuses on the way of translating legal contracts to machine-readable contracts while also making the newly created machine-readable contract automatically executable. As we aim to further incorporate the existing of a JCA into other smart contacts as a basis to decide if the processing of data is legal, we will focus in the following on the approach proposed by [13].

3 Using the JCA-SC to Ensure Legal Compliance for Data Processing in Smart Contracts

As mentioned, we use the proposed approach in [13] and analyze the possibility and the sufficiency of using the JCA smart contract (JCA-SC) as a base contract to other

contracts. The goal is to build a legally compliant system, which refuses data processing in a private permissioned blockchain system if no active and valid JCA is in place. The initial implementation of the JCA-SC is used from [13] which was built for the Hyperledger Fabric platform. Thus, we also used the Hyperledger Fabric platform for our prototype. Hyperledger Fabric itself is a permissioned blockchain for enterprises [21] and is one of the most used blockchain systems [2]. Within Hyperledger Fabric, two different kinds of nodes exist: Peer nodes, which hold onto the ledgers and smart contracts [22] and ordering nodes who order transaction and group them into new blocks [23] which are then distributed. Further, Hyperledger Fabric introduced the channel concept, which allows us to create "subnets" which can only be accessed by a selected and configured set of network members [24]. Note, that each channel has its own, independent blockchain, meaning that, as a single peer can be part of multiple channels, a single peer also holds onto multiple blockchains.

To evaluate our proposed smart contract combination from a technical point of view, we make use of the existing Hyperledger Fabric smart contract example *fabcar*, representing a car selling contract. We modified the fabcar smart contract in a way, that, before any processing of data takes place, the JCA-SC is called to verify the existing of a JCA. In figure 1 the sequence diagram shows how the actor interacts with the fabcar contract and how the fabcar contract itself interacts with our JCA-SC. The actor first needs to initialize the fabcar contract in which a default set of cars is stored on the ledger. Before data is processed, i.e. written to the ledger, the JCA-SC is called, checking if an active and valid JCA is in place. The returned result by the JCA-SC is then checked by the calling fabcar smart contract. If the returned result is positive, i.e. the JCA-SC confirmed an existing and accepted JCA, the init function of the fabcar smart contract will continue the data processing by initializing the ledger and will return a success message to the actor. In case the returned result is negative, i.e. the JCA-SC states that no JCA exists or that the JCA is not yet accepted by the required parties, the init method of the fabcar smart contract will abort and an error message is returned to the actor. By aborting the init method, any data processing is stopped as no legal certainty exist, based on the JCA-SC evaluation.

We found that the integration, i.e. the calling of the JCA-SC from the existing fabcar contract to be considered simple. This is due to the fact, that the Hyperledger Fabric system explicitly encourages developers to integrate and connect different smart contracts, providing the necessary functions and features. However, a major drawback is the mentioned integration which must be done manually by the developer. This means, that at every method of the fabcar contract, which processes data, a call to the JCA-SC must be implemented. Therefore, possible repetitive development and code duplicities are to be expected. Note that the sequence diagram only shows the sequence for the ledger initialization but is similar for other methods within the fabcar contract. Abstraction and reusing code will help to reduce the possible code duplicities.

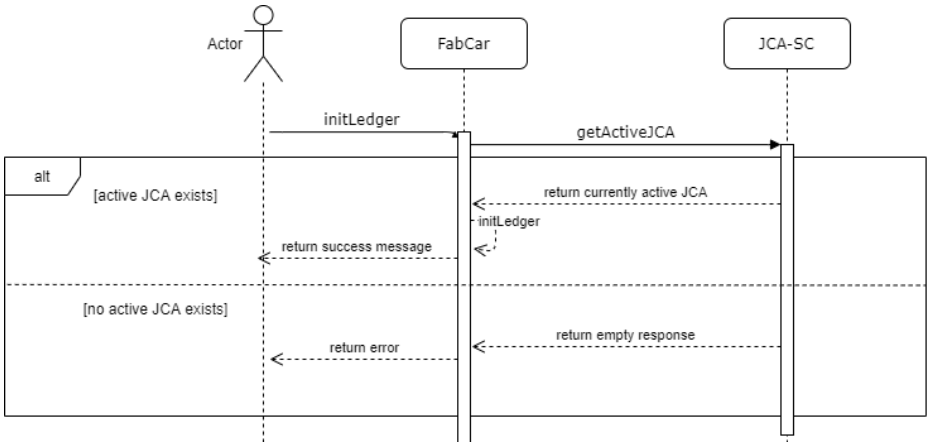

Figure 1. Sequence diagram combining FabCar contract and the JCA

4 On GDPR Enforcing Blockchains

The simple example above shows the general feasibility of combining a GDPR related smart contract, in this case, the JCA-SC, and contracts dealing with actual business logic. Manual integration can be considered error-prone like any other manual process. Therefore, it is next to discuss, if the integration of such features directly into the core functionality of a given blockchain, e.g. Hyperledger Fabric, is possible. Considering Hyperledger Fabric, such integration could take place in the Contract Interface in which several utility features are already implemented to ease the development of smart contracts so that the developer can focus on the actual business logic. Further, it must be evaluated if a general concept of such integration can be identified and then be applied to other blockchain systems as well. This exposes further possible new research directions, by shifting the focus of GDPR and blockchain from a perspective of problems (e.g. erasure of personal data in blockchains) towards the perspective of possibilities to further enforce GDPR and legal regulations in general. This could lead to legally compliant and compliance enforcing blockchain systems. Another use case for such smart contracts could be the digitization of *Standard Contractual Clauses* which gaining attention after the judgment of the Court of Justice of the European Union invalidates the EU-US Data Protection Shield [25]. In general, a combination of existing work towards GDPR enforcing blockchain-based approaches must be evaluated. The mentioned personal data management platform, for example, could be connected to the emerging research field of redactable blockchains [6–10]. It could be analyzed if a revoke of consent from the data subject via a respective system could trigger a block change if personal data is affected. Further, it can be evaluated if the JCA-SC can be enhanced in a way that it can automatically verify specific terms defined within the JCA. The work by [20] could serve as a starting point for such research. The proposed approach and ideas presented in this paper should serve as a starting point, aiming to design compliant and GDPR enforcing blockchain systems.

References

[1] X. Xu *et al.*, "A Taxonomy of Blockchain-Based Systems for Architecture Design," in *ICSA 2017: 2017 IEEE International Conference on Software Architecture : proceedings : 3-7 April 2017, Gothenburg, Sweden*, Gothenburg, Sweden, 2017, pp. 243–252. Accessed: Mar. 7 2019.

[2] G. Hileman and M. Rauchs, "GLOBAL BLOCKCHAIN BENCHMARKING STUDY," Cambridge Centre for Alternative Finance, 2017. Accessed: Aug. 22 2019. [Online]. Available: https://www.ey.com/Publication/vwLUAssets/ey-global-blockchain-benchmarking-study-2017/$File/ey-global-blockchain-benchmarking-study-2017.pdf

[3] G. Fridgen, F. Guggenmoos, J. Lockl, A. Rieger, A. Schweizer, and N. Urbach, "Developing an Evaluation Framework for Blockchain in the Public Sector: The Example of the German Asylum Process," 2018. Accessed: Mar. 15 2019.

[4] J. Benet, *IPFS - Content Addressed, Versioned, P2P File System: (DRAFT 3).* [Online]. Available: https://github.com/ipfs/papers/raw/master/ipfs-cap2pfs/ipfs-p2p-file-system.pdf (accessed: Apr. 11 2019).

[5] G. Fridgen, N. Guggenberger, T. Hoeren, W. Prinz, and N. Urbach, "Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik," 2019. Accessed: Nov. 18 2020. [Online]. Available: https://www.bmvi.de/SharedDocs/DE/Artikel/DG/blockchain-grundgutachten.html

[6] G. Ateniese, B. Magri, D. Venturi, and E. Andrade, "Redactable Blockchain – or – Rewriting History in Bitcoin and Friends," in *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, Paris, Apr. 2017 - Apr. 2017, pp. 111–126.

[7] S. Farshid, A. Reitz, and P. Roßbach, "Design of a Forgetting Blockchain: A Possible Way to Accomplish GDPR Compatibility," in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019.

[8] M. Florian, S. Henningsen, S. Beaucamp, and B. Scheuermann, "Erasing Data from Blockchain Nodes," in *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS & PW)*, Stockholm, Sweden, Jun. 2019 - Jun. 2019, pp. 367–376.

[9] A. Marsalek and T. Zefferer, "A Correctable Public Blockchain," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, Rotorua, New Zealand, Aug. 2019 - Aug. 2019, pp. 554–561.

[10] H. Precht and J. Marx Gómez, "REDACTABLE BLOCKCHAIN – LEVERAGING CHAMELEON HASH FUNCTIONS FOR A GDPR COMPLIANT BLOCKCHAIN," in *Konferenzband zum Scientific Track der Blockchain Autumn School 2020*, Mittweida, 2020, pp. 66–70.

[11] N. B. Truong, K. Sun, G. M. Lee, and Y. Guo, "GDPR-Compliant Personal Data Management: A Blockchain-Based Solution," *IEEE Trans.Inform.Forensic Secur.*, vol. 15, pp. 1746–1761, 2020, doi: 10.1109/TIFS.2019.2948287.

[12] Vargas and Juan Camilo, “Blockchain-based consent manager for GDPR compliance,” in *Open Identity Summit 2019*, 2019, pp. 165–170.
[13] T. Janicki and H. Precht, “Smart-Contract-basierter Joint Controllership Agreements in privaten Blockchains,” in *Den Wandel begleiten - IT-rechtliche Herausforderungen der Digitalisierung*, 2020.
[14] T. Janicki and D. Saive, “Privacy by Design in Blockchain-Netzwerken: Verantwortlichkeit und datenschutzkonforme Ausgestaltung von Blockchains,” *ZD • Zeitschrift für Datenschutz*, pp. 251–256, 2019.
[15] S. Gierschmann, “Gemeinsame Verantwortlichkeit in der Praxis – Systematische Vorgehensweise zur Bewertung und Festlegung,” *ZD • Zeitschrift für Datenschutz*, pp. 69–73, 2020.
[16] C. Wirth and M. Kolain, “Privacy by BlockChain Design: A BlockChain-enabled GDPR-compliant Approach for Handling Personal Data,” 2018.
[17] H. Precht and D. Saive, “Compliant Programming - Juristen in der agilen Softwareentwicklung,” in *Tagungsband Herbstakademie 2019*, 2019, pp. 581–595. [Online]. Available: https://beck-online.beck.de/?vpath=bibdata/zeits/DSRITB/2019/cont/DSRITB.2019.595.1.htm
[18] N. Szabo, *Smart Contracts: Building Blocks for Digital Markets.* [Online]. Available: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (accessed: May 12 2020).
[19] J. Mattila, “The Blockchain Phenomenon: The Disruptive Potential of Distributed Consensus Architectures,” *ETLA Working Papers*, no. 38, 2016. [Online]. Available: http://pub.etla.fi/ETLA-Working-Papers-38.pdf
[20] L. Cervone, M. Palmirani, and F. Vitali, “The Intelligible Contract,” in *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2020.
[21] Hyperledger Fabric, “Hyperledger Fabric: Open, Proven,Enterprise-grade DLT,” 2020. Accessed: May 13 2020. [Online]. Available: https://www.hyperledger.org/wp-content/uploads/2020/03/hyperledger_fabric_whitepaper.pdf
[22] Hyperledger Fabric, *Peers.* [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.0/peers/peers.html (accessed: May 13 2020).
[23] Hyperledger Fabric, *Orderer.* [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.0/orderer/ordering_service.html (accessed: May 13 2020).
[24] Hyperledger Fabric, *Channels.* [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/channels.html (accessed: May 13 2020).
[25] Court of Justice of the European Union, *The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield*. Luxembourg, 2020. Accessed: Nov. 26 2020. [Online]. Available: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf