# How to develop a GDPR-compliant blockchain solution for cross-organizational workflow management: evidence from the German asylum procedure

**Florian Guggenmos, Jannik Lockl, Alexander Rieger, Annette Wenninger, Gilbert Fridgen**

**Angaben zur Veröffentlichung / Publication details:**

Guggenmos, Florian, Jannik Lockl, Alexander Rieger, Annette Wenninger, and Gilbert Fridgen. 2020. "How to develop a GDPR-compliant blockchain solution for cross-organizational workflow management: evidence from the German asylum procedure." In *Proceedings of the 53rd Hawaii International Conference on System Sciences, HICSS, Maui, Hawaii, USA, January 7-10, 2020*, edited by Tung Bui. AISeL. https://doi.org/10.24251/hicss.2020.492.

# How to Develop a GDPR-Compliant Blockchain Solution for Cross-Organizational Workflow Management: Evidence from the German Asylum Procedure

Florian Guggenmos
FIM Research Center, University of Bayreuth
Project Group Business & Information Systems Engineering of the Fraunhofer FIT
florian.guggenmos@fit.fraunhofer.de

Annette Wenninger
FIM Research Center, University of Bayreuth
Project Group Business & Information Systems Engineering of the Fraunhofer FIT
annette.wenninger@fim-rc.de

Alexander Rieger
FIM Research Center, University of Augsburg
Project Group Business & Information Systems Engineering of the Fraunhofer FIT
alexander.rieger@fim-rc.de

Gilbert Fridgen
FIM Research Center, University of Bayreuth
Project Group Business & Information Systems Engineering of the Fraunhofer FIT
gilbert.fridgen@fit.fraunhofer.de

Jannik Lockl
FIM Research Center, University of Bayreuth
Project Group Business & Information Systems Engineering of the Fraunhofer FIT
jannik.lockl@fit.fraunhofer.de

## Abstract

*Blockchain technology has the potential to resolve trust concerns in cross-organizational workflows and to reduce reliance on paper-based documents as trust anchors. Although these prospects are real, so is regulatory uncertainty. In particular, the reconciliation of blockchain with Europe's General Data Protection Regulation (GDPR) is proving to be a significant challenge. We tackled this challenge with the German Federal Office for Migration and Refugees. Here, we explain how we used Action Research to guide the Federal Office in creating a GDPR-compliant blockchain solution for the German asylum procedure. Moreover, we explain the architecture of the Federal Office's solution and present two design principles for developing GDPR-compliant blockchain solutions for cross-organizational workflow management.*

## 1. Introduction

Within organizational boundaries, centralized workflow management systems have proven highly effective at increasing efficiency and reducing costs [23, 37]. However, beyond these boundaries, workflow management becomes challenging as mutual distrust often prevents the delegation of workflow governance to a central authority [23].

It has been proposed that the use of blockchain technology could ease these trust concerns [27]. Blockchains are distributed databases that use peer-to-peer protocols and cryptographic hash functions to propagate and store data in a tamper-resistant and consistent manner among the participants of a blockchain network [5, 16]. These properties allow the participants of a blockchain network to establish a "shared truth" without the need for a central authority [5].

Specifically, blockchain could increase the transparency of cross-organizational workflows and reduce the use of paper-based documents as trust anchors [27]. Although these prospects are real, regulatory uncertainties continue to hinder the adoption of blockchain-based workflow management [18]. These uncertainties include those arising from Europe's General Data Protection Regulation (GDPR). The GDPR codifies several rights of data subjects, such as the right to rectification and the right to erasure of their data. Moreover, it demands transparent responsibility for compliance with the

URI: https://hdl.handle.net/10125/64234
978-0-9981331-3-3

GDPR and bars processing of personal data without a lawful basis.

These requirements conflict with several of blockchain's properties. In particular, the right to erasure and rectification, and the GDPR's requirement that data controllers can be identified and held to account, present challenges for blockchain-based solutions [20].

In this paper, we argue that these conflicts can be resolved through a combination of organizational means and a three-layered architecture that enables rectification and erasure. Our arguments draw on learnings from our involvement in an ongoing blockchain project with Germany's Federal Office for Migration and Refugees (BAMF), which seeks to introduce a blockchain-based solution for the management of Germany's asylum procedure [13].

In particular, we outline what we learned in the course of three Action Research (AR) cycles that we used to guide the BAMF towards a GDPR-compliant blockchain solution. We also discuss how the architecture facilitates rectification and erasure of personal data, and present two actionable design principles for designing GDPR-compliant solutions in general and for cross-organization workflow management in particular.

The paper proceeds as follows: In section 2, we provide theoretical background on blockchain technology, the GDPR, and alternatives to reconcile the two. In Section 3, we describe our use of AR and the BAMF's blockchain project. Section 4 details the three cycles of our AR approach and discusses the architecture. In Section 5, we present and discuss the design principles we drew from the BAMF case. Section 6 concludes.

## 2. Theoretical background

Blockchain technology offers an innovative approach to data management. Instead of relying on a single trustworthy keeper, blockchain networks manage data by network consensus.

In many instances, this data is personal, i.e. it can be used to identify a natural person. In the European Union, processing of personal data has to comply with the binding rules of the GDPR. Several of these rules are challenging to meet, such as the need for clear responsibilities in the blockchain network, the establishment of lawful bases for processing, and the observance of the right to rectification and erasure.

### 2.1. Blockchain

In 2008, Nakamoto [26] conceived blockchain as a distributed digital ledger for Bitcoin transactions [3, 5]. Since these modest conceptual beginnings, researchers and practitioners have added various features, and developed blockchain-based solutions for cross-organizational workflow management [14], supply chain records [17, 25], security and privacy in the context of the Internet of Things [10, 32], finance and assurance [21], social business [33], and governmental services, as for example in Estonia [24] and Dubai [1].

Condos et al. [8] describe a blockchain as an electronic registry for digital records, events, and transactions, which is managed by the participants of a distributed computer network. In conceptual terms, a blockchain is a decentralized database that validates and stores data in so-called blocks. Consensus mechanisms order new blocks in an ever-expanding chain in order to ensure integrity and tamper-resistance [7, 29]. This chain is stored redundantly with each participant (technically called 'nodes') in the blockchain network, and new blocks are propagated throughout the network via peer-to-peer protocols [16].

From a more technical perspective, each block contains validated and structured data, and integrity is afforded by cryptographic hash functions. Appending a new block requires the calculation of the hash value of the data in the new block ($n$) and the hash value of the previous block ($n-1$). As such, the hash value of block $n$ includes the recursive hashes of all previous blocks [33]. Consensus mechanisms allow the blockchain network to agree on the validity and the order of the data in a block, and the correct order of the blocks [33]. Depending on the specific blockchain, technology (e.g., Bitcoin, Ethereum, Hyperledger), blockchain developers can choose from a variety of consensus mechanisms, each of which provides a different level of security and latency, and requires more or less energy [7, 36].

Blockchain solutions may also differ in terms of their assignment of read and write permissions (permissioned vs. permissionless blockchains), privacy (public vs. private blockchains), centralization, and efficiency [7, 28, 36]. The Bitcoin-Blockchain is a typical example of a public, permissionless blockchain. Each participant can download the blockchain, read all transactions, submit new transactions, and mine new blocks. In contrast, a private blockchain allows only verified members to see the stored data. Most private blockchains are also permissioned. This means that the network can decide who will become a new member and who can submit,

write, and read the information on the blockchain. Because this control requires that the identities of all network participants are known, a permissioned blockchain is less anonymous. Hyperledger is a typical example of a private, permissioned blockchain.

## 2.2. The General Data Protection Regulation

The GDPR standardizes the rules for the processing of personal data by both private and public data processors throughout the member states of the European Union (EU). It aims to allow data subjects to hold controllers and processors of their data to account, and it enshrines privacy by design and by default. At the same time, it aims to foster the free movement of personal data across the EU member states.

The GDPR applies to any act of processing any information relating to an identified or identifiable natural person in the EU, and to any such act by a data processor operating in the EU. It builds on a range of principles, as outlined in Article 5. Most importantly, it outlaws any processing of personal data unless the processor has a lawful basis, such as documented consent by the data subject or if the processing is required to meet contractual and legal obligations.

In particular, the GDPR strengthens the rights of data subjects (Chapter 3, Articles 12-23 GDPR). These rights include, among others, the right to rectification (Article 16) and the right to erasure (Article 17) [15].

## 2.3. Reconciliation of blockchain with the GDPR

Reconciling the processing of personal data through a blockchain network and the demands of the GDPR poses three essential challenges.

Firstly, the GDPR demands that responsibilities for ensuring compliance are clearly identified and designated, particularly when several parties jointly control the processing of personal data. Establishing these responsibilities is often not easy, especially if the blockchain network is public and permissionless. Secondly, the GDPR prohibits the processing of data unless, among others, this has been explicitly authorized by the subject or is required to fulfill obligations under law or contract (lawfulness of processing). However, establishing a lawful basis for each act of data processing in a blockchain network can be particularly cumbersome. The third challenge is the reconciliation of the rights to rectification and erasure with blockchain's premise of tamper-resistant on-chain storage. From a legal perspective, these challenges could be addressed using three different approaches [12]:

First, in the "central authority" approach, the network nominates a central authority. This authority may consist of a single participant of the blockchain network or a group of participants. The central authority assumes responsibility for compliance with the GDPR, establishes rights of network participants, and creates legal agreements for data processing with the nodes. The authority also secures the lawful bases for data processing and handles any related matters. If the blockchain network only processes the personal data of network participants, the central authority would have to create contracts with each network participant. If the network processes the personal data of third parties, the central authority must also secure the lawful basis for the processing of said third party data.

The right to rectification can be observed by submitting a rectification transaction to the blockchain. The right to erasure of personal data is waived by way of contract between the central authority and the network's participants, and affected third parties if necessary. In case any of these contracts become void, the blockchain may have to be modified.

Second, in the "shared responsibility" approach, all participants in the blockchain network jointly assume responsibility for GDPR compliance. The lawful basis for the processing of personal data relating to network participants and/or third parties is ideally assured through mutual contract. As in the "central authority" approach, the right to rectification is observable through rectification transactions, and the right to erasure is waived by way of contract. Again, any of the contracts becoming void can require the modification of the blockchain.

Third, in the "pseudonymization" approach, data on the blockchain is pseudonymized so that it only qualifies as personal data to those participants who possess certain additional information that allows attribution of the data to a natural person. Only those participants who possess the additional information required for attribution are controllers. When these controllers jointly determine the purposes and means of processing the pseudonymized data and the data required for attribution, they are joint controllers. At this point, they need to establish, through a joint control arrangement, their respective responsibilities for compliance with the GDPR and for establishing lawful bases for data processing. Otherwise, they can create data processing agreements to establish clear responsibilities for compliance. They can uphold the right to rectification through rectification transactions and the right to erasure by eliminating the additional information – that is, by depriving themselves of the

ability to attribute data to specific individuals. As such, the "pseudonymization" approach is considerably less risky from a legal perspective but requires a solution architecture which ensures that the additional information required for attribution can be securely shared and reliably eliminated.

## 3. Research approach

We chose a participatory action research approach to guide the BAMF's blockchain project. In particular, we held frequent functional and technical workshops to pinpoint problems, develop solutions, and foster reflective understanding. We also participated in developer, regular stand-up, and management meetings.

### 3.1. Case description

In Germany, asylum procedures require close collaboration and the exchange of information between various organizations at the municipal, state, and federal levels. Meanwhile, the exchange of certain data still takes place using paper records, which, in some cases, is still considered to be a more secure method of information sharing.

Although various digitalization projects have been effective in reducing paper-based communication and have substantially increased the efficiency of procedures, some of these projects have also introduced new challenges. Most prominent among these challenges is the management of the Central Register of Foreign Nationals (AZR), Germany's centralized database of information on foreign nationals in Germany. The AZR stores data on more than 26 million foreign nationals and grants more than 14,000 authorities access to read and write in these records.

The size of the AZR means that use often proves cumbersome, especially when it comes to logging, and informing users of data updates by other users. Moreover, the AZR is vulnerable to data quality issues because many updates are manual and many authorities do not use the AZR as their primary database. Although data security considerations are paramount, the AZR's centralized design translates into elevated vulnerability against failure and attacks. Legally, the AZR is bound to the provisions of a detailed AZR law. While this law provides a solid legal foundation, it also reduces the AZR's flexibility as many technical updates require a formal legislative process.

These complexities have encouraged the BAMF to explore a decentralized alternative for cross-organizational workflow management that would not require the extension of the AZR. After a preliminary evaluation, the BAMF narrowed down its technological options and decided to evaluate the prospects of blockchain technology in a Proof-of-Concept (PoC).

Over the course of the PoC project, the BAMF created a blockchain prototype for a simplified asylum procedure involving three authorities. The prototype used blockchain to log and propagate the completion of essential steps in the procedure. Moreover, an IT provider working for the BAMF coded the simplified asylum procedure into a smart contract to allow for automated monitoring of the workflow and automated triggering of subsequent process steps.

Based on their evaluation of this prototype, the BAMF put forward a case for the broader adoption of blockchain in the asylum procedure. This case rests on the premise that Germany's federal system severely limits centralized governance of asylum procedures. In particular, the German asylum procedure requires a solution that minimizes the redistribution of control and facilitates multilateral coordination.

Effective multilateral coordination, on the other hand, requires new process logs to be swiftly disseminated to all organizations so that each may initiate coordinative actions as required. Blockchain technology provides precisely this functionality and allows participants in the blockchain network to work with a "shared truth". Moreover, the procedure's many cross-organizational handovers require a high degree of data integrity. While blockchain cannot ensure the accuracy of the propagated process logs, it can ensure their consistency and availability for later process forensics.

Based on these arguments, the BAMF decided to advance its blockchain efforts and test the technology in a pilot project. Due to the complexity of the German asylum procedure, the BAMF limited the scope of its pilot project to two authorities (the BAMF and the Saxony's central immigration authority (LDS), Germany) and the AnkER procedure in Dresden, Saxony. The AnkER procedure is a particular instance of the German asylum procedure that clusters three essential elements of the procedure at one facility in order to increase efficiency: arrival (German: Ankunft), decision (Entscheidung), and return (Rückkehr). Figure 1 presents a schematic snapshot of the AnkER procedure and illustrates the mutual dependence of the BAMF and the LDS in managing asylum applicants.

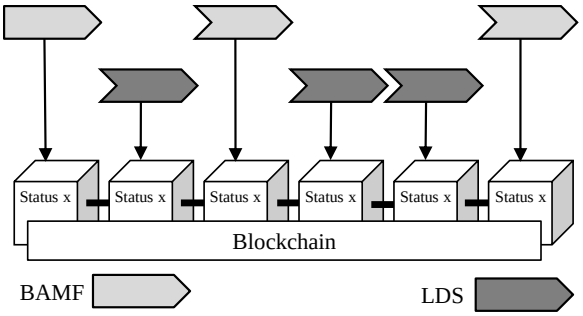


**Figure 1.** Schematic view of the use of blockchain in the pilot project

Although the BAMF had already emphasized privacy-by-design in the prototype, the use of actual personal data in the pilot required detailed consideration and observation of the GDPR's requirements.

The BAMF opted for a "pseudonymization" solution, as it deemed the collection of waivers from all affected third parties – that is, the asylum applicants – practically and legally impossible. It thus drafted an agreement with the LDS to set out the roles and responsibilities for joint control, as required by the GDPR. The BAMF also designed an architecture that enables both the separate sharing of process information required for effective cross-organizational workflow coordination and the sharing of information that allows the attribution of the process information to an asylum applicant. In particular, the pilot's architecture involves the use of so-called privacy services for the safe storage and exchange of the information required for attribution – that is, the mapping of a pseudonymous blockchain identifier to the specific IDs in the authorities' other databases.

### 3.2. Action research

The guidance we offered the BAMF followed an AR approach. AR was first introduced by Lewin in 1946 [19] and describes a cyclical process to investigate the organizational implications of theoretically derived practices [4, 9, 22]. AR intends that researchers cooperate with practitioners to understand and solve organizational issues, report and abstract the knowledge gained, and derive relevant implications for theory and future research [31]. AR is used in many contexts as organizational issues are often complex and challenging to solve [2]. In contrast to observational case studies, practitioners remain continuously aware of the presence of the researcher, who actively engages in the role of a consultant or organizational member, for example, by developing models and methods or giving decisive advice based on knowledge and theories relevant to practice [2, 4, 31]. Consequently, AR generates practical as well as theoretical outcomes.

Rapoport [30] and Evered [11] describe AR as an iterative five-stage cycle. Each cycle starts with the identification or definition of the problem (stage one, *diagnosing*). In a second step, the researcher creates a plan involving specific actions which will mitigate or solve the identified problem (stage two, *action planning*). In creating the plan, the researcher employs a theoretical framework which should explain why and how the planned actions will bring forth the desired change. Subsequently, at least one of the actions planned in stage two is executed (stage three, *action taking*). Upon execution, the researcher analyzes the consequences of the action and considers whether the action has had the intended effect (stage four, *evaluation*). In the last step, the researcher identifies general findings from stage four and communicates these findings to allow the resolution of the problem at hand and similar problems in other contexts (stage five, *specifying learning*). After performing stages one to five, the next cycle starts with stage one again. Typically, researchers traverse the AR cycle at least twice so that learning from the first cycle can be implemented in the *action planning*, *action taking*, and *evaluating* phases of the second cycle.

Following Yang et al. [34], we used a simplified AR approach with three cycles each involving three stages. In this simplified approach, stage one identifies and explains the problem (p*roblem*) whereas stage two (*intervention strategies*) combines the stages *action planning* and *action taking*, and stage three (*reflection*) combines the stages *evaluation* and *specifying learning*.

In each cycle, we had a different focus. In cycle one, we conveyed the importance of privacy-sensitivity in designing the prototype's architecture. In cycle two, we encouraged a detailed legal analysis in order to evaluate the prototype's compliance with the GDPR. In cycle 3, we aided the BAMF in creating a fully GDRP-compliant solution.

Empirically, we based the problem analysis and reflection stages on a rich set of 19 semi-structured interviews with BAMF stakeholders and external blockchain experts, five workshops, several informal discussions, two expert reports, direct observations, as well as on secondary documentation.

## 4. A GDPR-compliant blockchain solution for the German asylum procedure

We conducted cycle one of our three action research cycles during the first half of the PoC, and

cycle two spanned the latter half of the PoC. We began cycle three with the start of the pilot.

### 4.1. Cycle 1: Design of a privacy-sensitive architecture

*Problem:* The German asylum procedure requires many authorities and public organizations at the municipal, state, and federal levels to collaborate closely and exchange various information. Most of this information is sensitive, and most of the data processed in the course of the procedure are personal. Moreover, switching between different media and paper-based forms of communication is common. As a result, information on procedure updates propagates slowly, and the parties involved often lack a shared level of information, which increases the risk of substantial errors such as unlawful repatriation. In order to address these issues, the BAMF had already explored options for a cross-organizational workflow system. This exploration process had established that neither an extension of the AZR nor the introduction of conventional workflow management with centralized process governance would effectively address the identified issues.

*Intervention strategies:* In a joint ideation workshop with the BAMF, we evaluated whether blockchain could be used to address the identified challenges and provide a workflow coordination solution for the German Asylum procedure. Based on the positive results of this evaluation, we encouraged the BAMF to advance its exploration to a PoC project. Because of the sensitive and personal nature of many of the data, we suggested that the BAMF should be especially sensitive to data privacy.

During the PoC, the BAMF created a blockchain prototype for a simplified asylum procedure. The prototype used blockchain to log and propagate the completion of essential steps in the procedure. In order to foster privacy by design, we suggested that the prototype should minimize the amount of information stored on the blockchain, and preserve the data sovereignty of individual authorities. The BAMF heeded our advice and designed a three-layer architecture that stored a minimum amount of information on the blockchain (layer one – blockchain layer) and relied on blockchain adapters for efficient requests and off-chain sharing of data (layer two – adapter layer). Only in response to certain triggers would the blockchain adapters pull data from the authorities' databases and workflow management systems (layer three – existing systems layer).

In particular, the adapters respond to specific actions in the workflow management systems and communicate the data / status changes to the blockchain as events. Each event has a status, a time-stamp, the ID of the authority that created the status update, and the AZR ID of the asylum seeker concerned. The adaptors submit these events to the blockchain. Once stored on the blockchain, the events can trigger the actions of a smart contract that allows the automated monitoring of the workflow and the automated triggering of subsequent process steps.

As the PoC emphasized data privacy, the BAMF only worked with dummy data. Moreover, the BAMF decided to use a private permissioned blockchain that would allow fine-grained identity and access management.

*Reflection:* The PoC demonstrated that a blockchain could provide the essential features of cross-organizational workflow coordination while adhering to important privacy-by-design principles. Moreover, a blockchain solution could maintain the asylum procedure's decentralized workflow governance and ensure that each authority maintained guardianship over its data.

### 4.2. Cycle 2: Detailed analysis of GDPR-compliance

*Problem:* During cycle 1, the BAMF focused primarily on the technical feasibility of a blockchain solution that was both effective and privacy-sensitive. However, the BAMF had designed its prototype without detailed consideration of data privacy regulations in general and the GDPR in particular.

*Intervention strategies:* In cycle 2, we thus encouraged the BAMF to analyze its prototype solution from a legal perspective. The BAMF again heeded our advice and sought external legal advice on the prototype from a renowned professor in the area of blockchain and data protection.

*Reflection:* From the legal analysis, it became evident that the prototype complied with data exchange regulation yet did not comply with the GDPR as the use of the AZR ID made all data on the blockchain personal data. However, the legal opinion indicated that a pseudonymization solution would resolve this problem.

### 4.3. Cycle 3: Design of a GDPR-compliant architecture

*Problem:* Because of the novelty of both the GDPR and blockchain, the BAMF could not resort to a best practice approach when designing a pseudonymization solution.

*Intervention strategies:* In order to mitigate the lack of best practices, we held several ideation and architectural refinement workshops. Moreover, the BAMF met with Germany's Federal Commissioner for Data Protection and Freedom of Information (BfDI). In a two-day workshop, the BAMF and experts from the BfDI discussed the prototype and how it could be made to comply with the GDPR.

These two measures lead to two essential modifications of the prototype's architecture:

One, the BAMF extended the adapter layer with a privacy service. This highly secure service maps pseudonymous Blockchain-IDs to the IDs used in the existing systems and repositories. Importantly, each authority has its own privacy service. Mapping information can be exchanged between privacy services to allow the receiving authority to attribute process updates.

Two, the project team developed a rectification and erasure concept. When rectification of on-chain data is required, the competent authority can submit a rectification transaction to the blockchain. When erasure of the on-chain data is required, for instance, because of time limits placed on the storage of personal data, the authorities can delete the mapping in the privacy service, meaning they can no longer identify the respective pseudonymous blockchain ID. In other words, the on-chain data is not deleted, but it is depersonalized.

*Reflection:* In the course of cycle three, the BAMF developed a fully functional pseudonymization solution.

### 4.4. Blockchain system architecture

Figure 2 illustrates a schematic view of the final GDPR-compliant architecture.

The architecture has three layers. Layer one represents the databases and workflow management systems of the participants of the blockchain network. Layer two, the adapter layer, holds the blockchain adapters and privacy services. The blockchain adapters connect the databases and systems on layer one to the blockchain on layer three. They control the submission of status updates to the blockchain. The privacy services map the authorities' specific identifiers to the pseudonymous identifiers used on the blockchain. Layer three holds the blockchain with the events. Similar to the prototype, each event has a status, a time-stamp, the ID of the authority that created the status update, and a pseudonymous ID that allows for the identification of asylum seekers only in conjunction with the privacy service.

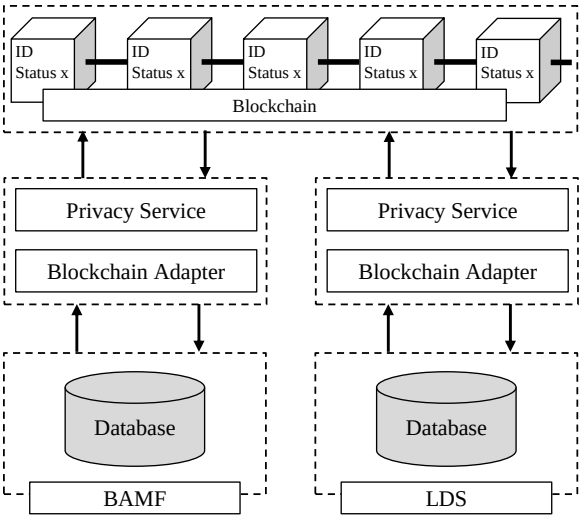


**Figure 2.** Schematic view of the GDPR-compliant architecture of the BAMF's blockchain solution

Technically speaking, the BAMF uses a Hyperledger Fabric blockchain and standardized interfaces (e.g., REST or Web3J) to connect the layers.

## 5. Design principles for GDPR-compliant blockchain design

Legally, blockchain solutions can be reconciled with the GDPR through a "central authority", a "shared responsibility", or a "pseudonymization" approach. In practical terms, the pseudonymization option may often be preferable as it seeks to observe the right to erasure through technical means, rather than to use a set of voidable contracts. However, this option requires significant design considerations. In the guidance we offered the BAMF, we identified two tentative design principles that can aid these considerations:

*Design Principle 1: Do not store personal data on a blockchain*

Blockchain's paradigm of tamper-resistant storage seems to jar profoundly with the right to rectification and erasure. As such, we encourage blockchain solution architects to keep personal data off-chain. Solutions exist in which tampering approaches would allow for the deletion of data stored on the blockchain layer [12]. Such an approach, however, would betray the idea of tamper-resistant storage. Consequently, this design principle may encourage the creation of a B2B blockchain network that does not process personal data – neither of the participants of the network nor of third parties.

*Design Principle 2: If a use case requires that data on the blockchain be attributable to a natural person, use a highly secure off-chain mapping architecture.*

Certain use cases, such as the one we explored with the BAMF, require that information propagated and stored on the blockchain can be attributed to a natural person. As Design Principle 1 also applies in these use cases, the information on the blockchain must not allow attribution without further information, and blockchain solution architects should employ a pseudonymization solution [12]. The information required for attribution, such as a mapping of abstract blockchain IDs with specific IDs, has to remain off-chain and should be propagated using secure information channels. With such a solution, data controllers can "rectify", through the propagation of rectification transactions, and they can "erase", through the deletion of the information required for attribution.

## 6. Conclusion

Centralized workflow management systems increase efficiency and reduce cost in contexts that permit centralized workflow governance. However, such systems are impractical in cross-organizational settings which prevent the delegation of workflow governance to a central authority. Blockchain-based solutions could be a promising alternative in these settings because they emphasize decentralized governance. However, the reconciliation of blockchain-based solutions with the GDPR is a significant challenge.

In this paper, we discuss how the BAMF realized this reconciliation. Moreover, we detail the GDRP-compliant solution that the BAMF developed for the German asylum procedure and present two actionable design principles for GDPR-compliant design of blockchain solutions in the area of cross-organizational workflow management.

From a practical angle, our study illustrates how blockchain solutions can meet the requirements of the GDPR. From a theoretical angle, we contribute to the growing field of IS research on the management of data privacy requirements [6, 35].

Naturally, the BAMF's architecture may not be the best solution in other contexts. Moreover, many elements of the architecture have yet to demonstrate their suitability for large-scale deployment beyond the two authorities involved in the BAMF's pilot setting. We also caution against viewing the architecture as a stand-alone solution. It requires complementary organizational measures, such as the creation of an arrangement on the division of responsibilities among the joint controllers to establish full compliance with the GDPR.

In sum, our study supports the argument that blockchain and the GDPR are not jarring opposites, and that we should continue the exploration and development of blockchain-based solutions for cross-organizational workflow managment. The next essential step in this journey will be to establish standards and reference architectures that ensure the interoperability of various blockchain technologies and solutions.

## 7. References


[1] Alketbi, A., Nasir, Q. and M.A. Talib, "Blockchain for government services—Use cases, security benefits and challenges", in 2018 15th Learning and Technology Conference. IEEE.

[2] Avison, D.E., R.M. Davison, and J. Malaurent, "Information systems action research: Debunking myths and overcoming barriers", Information & Management, 55(2), 2018, pp. 177–187.

[3] Avital, M., R. Beck, J.L. King, M. Rossi, and R. Teigland, eds., Jumping on the Blockchain Bandwagon: Lessons of the Past and Outlook to the Future, ICIS Proceedings, 2016.

[4] Baskerville, R. and M.D. Myers, "Special issue on action research in information systems: Making IS research relevant to practice: Foreword", MIS Quarterly, 2004, pp. 329–335.

[5] Beck, R., C. Müller-Bloch, and J.L. King, "Governance in the Blockchain Economy: A Framework and Research Agenda", Journal of the Association for Information Systems, 19(10), 2018.

[6] Chanson, M., A. Bogner, D. Bilgeri, E. Fleisch, and F. Wortmann, "Privacy-Preserving Data Certification in the Internet of Things: Leveraging Blockchain Technology to Protect Sensor Data", Journal of the Association for Information Systems, 2019.

[7] Christidis, K. and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things", IEEE Access, 4, 2016, pp. 2292–2303.

[8] Condos, J., W.H. Sorrell, and S.L. Donegan, Blockchain technology: Opportunities and risks, 2016.

[9] Davison, R.M., M.G. Martinsons, and C.X.J. Ou, "The roles of theory in canonical action research", MIS Quarterly, 2012, pp. 763–786.

[10] Dorri, A., S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home", 2017 IEEE International Conference on

Pervasive Computing and Communications Workshops (PerCom Workshops), 2017, pp. 618–623.
[11] Evered, R.D., "An Assessment of the Scientific Merits of Action Research Gerald 1. Susman and", Administrative science quarterly, 23(4), 1978, pp. 582–603.

[12] Fridgen, G., N. Guggenberger, T. Hoeren, W. Prinz, and N. Urbach, "Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik", https://www.bmvi.de/SharedDocs/DE/Anlage/DG/blockchain-gutachten.pdf?__blob=publicationFile, 2019.

[13] Fridgen, G., F. Guggenmos, J. Lockl, A. Rieger, and N. Urbach, "Supporting communication and cooperation in the asylum procedure with Blockchain technology– A proof of concept by the Federal Office for Migration and Refugees", 2019.

[14] Fridgen, G., S. Radszuwill, N. Urbach, and L. Utz, "Cross-organizational workflow management using blockchain technology-towards applicability, auditability, and automation", Proceedings of the 51st Hawaii International Conference on System Sciences, 2018, pp. 3507–3516.

[15] General Data Protection Regulation: Regulation (EU) 2016/679, 27 April 2016.

[16] Glaser, F., "Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis", Proceedings of the 50th Hawaii International Conference on System Sciences, 2017, pp. 1543–1552.

[17] Korpela, K., J. Hallikas, and T. Dahlberg, "Digital Supply Chain Transformation toward Blockchain Integration", in Proceedings of the 50th Hawaii International Conference on System Sciences, Waikoloa, Hawaii, USA. 2017.

[18] Lacity, M.C., "Addressing key challenges to making enterprise blockchain applications a reality", MIS Quarterly Executive, 17(3), 2018, pp. 201–222.

[19] Lewin, K., "Action research and minority problems", Journal of social issues, 2(4), 1946, pp. 34–46.

[20] Lyons, T., L. Courcelas, and K. Timsit, "Blockchain and the GDPR", https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf.

[21] Mansfield-Devine, S., "Beyond Bitcoin: using blockchain technology to provide assurance in the commercial world", Computer Fraud & Security, 2017(5), 2017, pp. 14–18.

[22] Mathiassen, L., M. Chiasson, and M. Germonprez, "Style Composition in Action Research Publication", MIS Quarterly, 36(2), 2012, pp. 347–363.

[23] Mendling, J., I. Weber, W.V.D. Aalst, J.V. Brocke, C. Cabanillas, F. Daniel, S. Debois, C. Di Ciccio, M. Dumas, S. Dustdar, A. Gal, L. García-Bañuelos, G. Governatori, R. Hull, M. La Rosa, H. Leopold, F. Leymann, J. Recker, M. Reichert, H.A. Reijers, S. Rinderle-Ma, A. Solti, M. Rosemann, S. Schulte, M.P. Singh, T. Slaats, M. Staples, B. Weber, M. Weidlich, M. Weske, X. Xu, and L. Zhu, "Blockchains for Business Process Management - Challenges and Opportunities", ACM Transactions on Management Information Systems (TMIS), 9(1), 2018, pp. 4–20.

[24] Mettler, M., "Blockchain technology in healthcare: The revolution starts here", in 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services. 2016.

[25] Min, H., "Blockchain technology for enhancing supply chain resilience", Business Horizons, 62(1), 2019, pp. 35–45.

[26] Nakamoto, S., "Bitcoin: A peer-to-peer electronic cash system", 2008.

[27] Pedersen, A.B., M. Risius, and R. Beck, "A Ten-Step Decision Path to DetermineWhen to Use Blockchain Technologies", MIS Quarterly Executive, 18(2), 2019.

[28] Peters, G.W. and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money", in Banking Beyond Banks and Money. 2016. Springer.

[29] Porru, S., A. Pinna, M. Marchesi, and R. Tonelli, "Blockchain-Oriented Software Engineering: Challenges and New Directions", in 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C). 2017. IEEE.

[30] Rapoport, R.N., "Three dilemmas in action research: with special reference to the Tavistock experience", Human relations, 23(6), 1970, pp. 499–513.

[31] Recker, J., Scientific research in information systems: a beginner's guide, Springer Science & Business Media, 2012.

[32] Sadique, K.M., R. Rahmani, and P. Johannesson, "Towards Security on Internet of Things: Applications and Challenges in Technology", Procedia Computer Science, 141, 2018, pp. 199–206.

[33] Schweizer, A., V. Schlatt, N. Urbach, and G. Fridgen, "Unchaining Social Businesses - Blockchain as the Basic Technology of a Crowdlending Platform", in Proceedings of the 38th International Conference on Information Systems, Y.J. Kim, R. Agrawal, and J.K. Lee, Editors, Seoul; South Korea. 2017.

[34] Yang, S.O., C. Hsu, S. Sarker, and A.S. Lee, "Enabling effective operational risk management in a financial institution: An action research study", Journal of Management Information Systems, 34(3), 2017, pp. 727–753.

[35] Yun, H., G. Lee, and D.J. Kim, "A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs", Information & Management, 56(4), 2019, pp. 570–601.

[36] Zheng, Z., S. Xie, H.-N. Dai, and H. Wang, "Blockchain Challenges and Opportunities: A Survey", Int. J. Web and Grid Services, 2016, pp. 1–25.

[37] Zyskind, G. and O. Nathan, "Decentralizing privacy: Using blockchain to protect personal data", 2015 IEEE Security and Privacy Workshops, 2015.