MIS Quarterly Executive

Building a Blockchain Application that Complies with the EU General Data Protection Regulation

Complying with the EU General Data Protection Regulation (GDPR) poses significant challenges for blockchain projects, including establishing clear responsibilities for compliance, securing lawful bases for processing personal data, and observing rights to rectification and erasure. We describe how Germany's Federal Office for Migration and Refugees addressed these challenges and created a GDPR-compliant blockchain solution for cross-organizational workflow coordination. Based on the lessons learned, we provide three recommendations for ensuring blockchain solutions are GDPR-compliant.[1,2]

Alexander Rieger
University of Augsburg
(Germany)
FIM Research Center

Florian Guggenmos
University of Bayreuth
(Germany)
Project Group Business & Information Systems Engineering of the Fraunhofer FIT

Jannik Lockl
University of Bayreuth
(Germany)
Project Group Business & Information Systems Engineering of the Fraunhofer FIT

Gilbert Fridgen
University of Luxembourg
(Luxembourg)
SnT - Interdisciplinary Centre for Security, Reliability and Trust

Nils Urbach
University of Bayreuth
(Germany)
Faculty of Law, Business, and Economics

The EU General Data Protection Regulation Poses Significant Challenges for Blockchain Projects

Blockchain technology provides an innovative means of fostering collaboration, especially in cross-organizational workflows. Blockchain solutions allow the organizations involved in the workflow to maintain control over their respective activities but, at the same time, enable them to establish a "shared and persistent truth" on the state of the workflow at any given time. This truth can act as a point of reference if conflicts need to be resolved at a later point. By extension, this allows the organizations to use updates on the blockchain as reliable

1 Carsten Sørensen is the accepting senior editor for this article.

2 We developed this article as part of an applied research project with Germany's Federal Office for Migration and Refugees. The authors would like to thank everyone involved for their support. We would also like to express our gratitude to Carsten Sørensen, Mary Lacity, Rajiv Sabherwal, and three anonymous reviewers for their guidance and comments, which considerably improved this article.

DOI: 10.17705/2msqe.00020

triggers for subsequent activities. Moreover, the continuous distribution of updates throughout the network means that these triggers are readily available. If required, smart contracts can also allow the automated activation of certain steps of the workflow and its monitoring. In simple terms, blockchain technology offers a promising alternative to centralized workflow management systems where the delegation of workflow governance to a central authority is not possible or desirable.[3]

However, when blockchain projects move beyond the proof-of-concept stage, they begin to encounter the limiting effects of regulations and legal barriers. Foremost among these is the European Union (EU) General Data Protection Regulation (GDPR).[4] The GDPR protects a "natural person"[5] from unregulated processing of their personal data and establishes rules governing the free movement of their personal data. It codifies several essential rights of natural persons, such as the right to have inaccurate personal data rectified, or completed if it is incomplete, and to have their personal data erased. Moreover, it establishes clear responsibilities for compliance with the regulation and prohibits the processing of personal data without a lawful basis, such as requiring explicit consent if the action is necessary to fulfill obligations of a law or contract.

At first glance, many of the GDPR requirements appear to conflict with the basic properties of blockchain technology. For instance, the technology does not envisage the data being erased at a later point. Moreover, the decentralized nature of blockchain networks seems to prevent the designation of clear responsibilities. Also, the need to obtain a lawful basis for processing personal data at each node appears daunting.

As we show in this article, however, these challenges can be resolved. We describe how the Bundesamt für Migration und Flüchtlinge (the BAMF—Germany's Federal Office for Migration and Refugees) created a GDPR-compliant blockchain solution for processing applications for asylum. (The German asylum procedure is described in Appendix A.) The key learnings from this project give rise to three recommendations for the management of GDPR requirements and the design of GDPR-compliant blockchain solutions. (Appendix B describes the research we conducted in preparing to write this article.)

A Brief Introduction to the EU General Data Protection Regulation

Data privacy has been an important focus of European lawmaking since the 1970s. A key multilateral milestone was the EU's 1981 signing of the Convention for the Protection of Individuals, which addressed the automatic processing of personal data. The most recent and comprehensive regulatory step was the passing of the General Data Protection Regulation in 2016, which took effect across all member states of the EU in May 2018.

The GDPR applies to any act of wholly or partially automated processing[6] of any information relating to an identified or identifiable natural person in the EU, and to any such act by a data controller[7] or a data processor[8] that operates on that person's behalf, in the European Union. Importantly, it relates not only to data that is obviously personal, such as names

3 For a detailed discussion on the prospect of using blockchains for the management of business processes and workflows, see Mendling, J. et al. "Blockchains for Business Process Management : Challenges and Opportunities," *ACM Transactions on Management Information Systems* (9:1), February 1, 2018, pp. 1-16.

4 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*, Council of the European Union, European Parliament; the full text of the GDPR is available at https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en. While the GDPR is an EU regulation, many global platforms and other cross-border firms observe its requirements.

5 The GDPR regulates the processing of information relating to an identified or identifiable natural person—i.e., an individual human being. It does not regulate the processing of information relating to legal persons.

6 As set out in Article 4(2) of the GDPR, the term "processing" encompasses a wide variety of conceivable actions, such as recording, storing, and disseminating data.

7 Article 4(7) of the GDPR defines a data controller as a "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 …."

8 Article 4(8) of the GDPR defines a data processor as a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

but also to data that, in combination with other means, can be used to identify a natural person.[9]

The GDPR aims to foster the free movement of personal data within EU member states by standardizing the rules for the processing of personal data by both private and public data controllers. It builds on six principles, including purpose limitation and data minimization, and enshrines privacy by design and by default. Importantly, it outlaws any processing of personal data unless the data controller has a lawful basis.

Chapter 3 of the GDPR also establishes the various rights of data subjects[10] (Articles 12 to 23). These rights include, among others, the right to rectification (Article 16)[11] and the right to erasure ("the right to be forgotten") (Article 17)[12]. This means that data subjects can hold controllers and processors of their data accountable, and violators can incur hefty fines. In particular, Article 83(5) of the GDPR prescribes administrative fines of up to €20 million ($22.29 million)[13] or, in the case of companies, up to 4% of total worldwide annual revenue from the preceding financial year, whichever is higher.

Reconciling Blockchain Solutions with the GDPR

Most guidelines on the management of GDPR requirements presuppose a single identifiable controller and skirt around the particularities of decentralized networks in general and blockchain technology in particular. Blockchain projects therefore face genuine challenges in observing the requirements of the GDPR. Chief among these challenges is the need to establish clear responsibilities for compliance, to secure lawful bases for processing personal data, and to comply with the rights to rectification and erasure.

Establishing Clear Responsibilities for Compliance. The GDPR requires that responsibilities for compliance with its articles are identified and designated, especially when several parties jointly determine the purposes and means of processing ("joint control").[14] For conventional databases, the establishment of responsibilities is comparatively easy. In blockchain networks, defining responsibility is often difficult. In particular, legal opinions differ as to which participants qualify as standalone controllers and which as joint controllers. The distinction is important because joint controllers are jointly accountable and have to create an arrangement that identifies each joint controller and determines their respective responsibilities, and that is transparent to the affected data subjects.[15]

Securing Lawful Bases for Processing Personal data. Article 5 of the GDPR specifies six lawful bases for processing personal data, including documented authorization by the data subject or processing that is required to fulfill obligations under law or contract;[16] without one of these lawful bases, a data controller cannot legally process personal data. Establishing lawfulness for each data-processing action in a blockchain network can be particularly

9 In particular, the GDPR also applies to data that allows attribution through the analysis of patterns of use and context. In many instances, this includes public keys. For more details on the resulting challenges, see Lyons, T., Courcelas, L. and Timsit, K. *Blockchain and the GDPR*, The European Union Blockchain Observatory and Forum, October 16, 2018, available at https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf.

10 The GDPR uses the term "data subject" as a synonym for any identified or identifiable natural person.

11 Article 16 of the GDPR grants each data subject "the right to obtain from the controller without undue delay the rectification of inaccurate personal data."

12 Article 17 of the GDPR states that an individual has "the right to obtain from the controller the erasure of personal data concerning him or her without undue delay" when one of the defined reasons applies.

13 Euro/dollar conversion rate as of October 2019.

14 The primary criterion for qualifying as joint controllers is the joint determination of the purpose of processing ("primacy of the purpose criterion"); simple participation in the determination of the means does not necessarily qualify a participant of a blockchain network as a joint controller. For a detailed discussion of joint controllership in the context of blockchains, see *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?,* European Parliamentary Research Service, July 2019, available at http://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

15 The national data protection authority of France (CNIL), for instance, considers participants of blockchain networks to be data controllers "when the … participant is a natural person and … the personal data processing operation is related to a professional or commercial activity" or "when the … participant is a legal person and … it registers personal data in a blockchain." When these controllers do not designate a single controller who determines the purposes and mean of processing, regulators and courts may easily decide to hold them accountable as joint controllers. The CNIL's detailed opinion is in *Blockchain: Solutions for a responsible use of the blockchain in the context of personal data*, 2018, available at https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf

16 Lawfulness has to be established for three essential processing steps: the submission of new data to the blockchain by a submitting participant; its validation, distribution, and replication by the nodes of the blockchain network; and its reading from the blockchain by another participant.

Table 1: Advantages and Disadvantages of the Central Authority, Shared Responsibility, and Pseudonymization Approaches

	Description (in terms of controlling and complying with the right to erasure)	Advantages	Disadvantages
Central Authority	• The network nominates a central authority that acts as the network's single controller • The right to erasure is waived by way of contracts between the central authority and the network's participants, and in consultation with affected third parties if necessary	• Easy identification of the data controller • Requires a less intricate solution architecture	• Requires centralized control over network rights • If any of the erasure contracts become void, the blockchain may have to be modified
Shared Responsibility	• All participants in the blockchain network act as joint controllers • The right to erasure is waived by way of mutual contracts between the network's participants, and in consultation with affected third parties if necessary	• Does not require centralized control over network rights • Requires a less intricate solution architecture	• There must be a legal basis for processing personal data for each participant • If any of the erasure contracts become void, the blockchain may have to be modified
Pseudonymization	• Data on the blockchain is pseudonymized; only those participants who possess the additional information required for attribution are (joint) controllers • The blockchain solution can comply with the right to erasure by eliminating the additional information	• Does not require centralized control over network rights • The right to erasure is upheld by design	• Requires an intricate solution architecture to ensure that the additional information required for attribution can be securely shared and reliably eliminated • The blockchain may have to be modified if there is inadvertent attribution from examining patterns of use or context (linkability risk) or any other inadvertent reversal of the pseudonymization (reversal risk)

burdensome. Moreover, any lawful basis may cease to exist or apply in the future (e.g., with the withdrawal of consent or amendment of the law). In these circumstances, storage of the relevant personal data is no longer permitted and the data must be erased.

Complying with the Rights to Erasure and Rectification. The GDPR states that data subjects can request that data controllers rectify their personal data if there are errors and erase the data once a lawful basis ceases to exist. This implies that modifications to data on a blockchain must be made on each copy of the blockchain.

Three Potential Approaches for Ensuring Blockchain Solutions Are GDPR-Compliant

From a data-privacy perspective, addressing the three challenges described above requires a combination of organizational and technical measures. We have identified three potential blockchain solution approaches—"central authority," "pseudonymization,"[17] and "shared responsibility."[18] Table 1 lists the advantages and disadvantages of these approaches, and we describe them below. To the best of our knowledge, there is no single best approach for each application and context. Moreover, the approaches are not comprehensively exhaustive, and some blockchain projects may identify other ways of ensuring they comply with the requirements of the GDPR.

Central Authority Approach. The central authority approach addresses conflicts between GDPR requirements and a blockchain solution through organizational measures and by delegating responsibility to a central authority. This authority may be a single participant in the blockchain network or a group of participants. The central authority assumes the role of the data controller and the responsibility for compliance with the GDPR. Moreover, it establishes the rights of network participants and creates, using a contract or another legal instrument, agreements for processing personal data with the operators of the blockchain nodes. The authority also secures the lawful bases for processing personal data and handles any related matters. When the blockchain network processes the personal data of network participants, the central authority has to create contracts with each network participant. When the network processes the personal data of third parties, the central authority must secure the lawful bases for processing the data of those third parties.

The right to erasure of personal data is waived by way of contracts between the central authority and the network's participants, and, if necessary, in consultation with affected third parties. If any of these contracts become void, the blockchain network must erase the personal data from the blockchain. This can be done in several ways. For instance, each node can remove the data from its block and recalculate all subsequent blocks. This recalculation can be documented in another blockchain. Another option is to use redactable[19] blockchains. The right to rectify data can be achieved through technical means by submitting a rectification transaction to the blockchain. More specifically, the original transaction is invalidated by the rectification transaction, but it remains on the blockchain.

The central authority approach is appropriate for blockchain solutions that permit the designation of a single data controller with far-reaching competencies.

Shared Responsibility Approach. The shared responsibility approach is very similar to the central authority approach but builds on the premise of sharing responsibilities among the participants of the blockchain network. All participants in the network act as joint controllers and establish an arrangement that sets out the respective responsibilities of each participant. The lawful basis for processing

17 Article 4(5) of the GDPR defines pseudonymization as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." Pseudonymization is different from anonymization, which renders personal data "anonymous in such a manner that the data subject is not or no longer identifiable." (Recital 26 of the GDPR).

18 For a comprehensive discussion of the three approaches, see Fridgen, G., Guggenberger, N., Hoeren, T., Prinz, W. and Urbach, N. *Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik*, (the management summary is in English), Bundesministeriums für Verkehr und digitale Infrastruktur, May 2019, available at https://www.bmvi.de/SharedDocs/DE/Anlage/DG/blockchain-gutachten.pdf?__blob=publicationFile.

19 For a discussion of redactable blockchains, see Ateniese, G., Magri, B., Venturi, D. and Andrade, E. "Redactable Blockchain – or – Rewriting History in Bitcoin and Friends", 2017 IEEE Symposium on Security and Privacy, May 11, 2017 pp. 111-126.

personal data relating to network participants and/or third parties is ideally ensured through mutual contracts. As with the central authority approach, the right to erasure is waived by way of contracts between the network's participants and, if necessary, with affected third parties. Again, the right to rectification can be achieved through rectification transactions.

The shared responsibility approach is appropriate for blockchain networks where all participants have lawful bases for processing all the personal data exchanged.

Pseudonymization Approach. As its name suggests, this approach is based on pseudonymizing the data on the blockchain so that it only qualifies as personal data when participants possess certain additional off-chain information that allows the data to be attributed to a natural person. Pseudonymization of the data can be achieved using encryption, cryptographic hash functions, or pseudonymous identifiers.[20] 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. As such, they need to establish, through a joint control arrangement, their respective responsibilities for compliance with the GDPR and for establishing lawful bases for processing personal data. Alternatively, they can create data processing agreements to establish clear responsibilities for compliance.

Controllers and processors can uphold the right to erasure by eliminating the additional information—that is, by depriving themselves of the ability to attribute data to specific individuals. This technical measure is considerably more reliable than an organizational measure based on waivers but requires a solution that ensures that the additional information needed for attribution can be securely shared and reliably eliminated. The process for rectification mirrors the central authority and shared responsibility approaches.

The pseudonymization approach is appropriate for blockchain networks where the designation of a central authority is not viable or desirable, and where not all participants have lawful bases for the processing of all the personal data exchanged.

20 In the first case, the additional information required for attribution is the decryption key. In the second case, the additional information is the unhashed information, and in the third case, the additional information required for attribution is the mapping of a pseudonymous identifier to a specific identifier.

Background of the Choice of Blockchain Technology for the German Asylum Procedure

In Germany, the asylum procedure involves close collaboration between various authorities at the municipal, state and federal levels, with the BAMF playing a pivotal central role because it handles and issues decisions regarding asylum applications. State-level migration authorities are responsible for the initial registration of asylum seekers, and for their eventual integration or repatriation. Several security agencies are involved in background checks; municipal governments generally handle housing, and various health authorities provide medical care.

Lessons Learned from Early Efforts to Introduce Centralized Support Systems for the Asylum Procedure

Federal separation of competencies prevents the delegation of workflow governance to a central authority, such as the BAMF. This separation also leads to a significant degree of variation between workflows, and complicates the creation of a common workflow model and the introduction of a conventional workflow management system.

One essential step in managing the resulting complexities was to transform the Central Register of Foreign Nationals (Ausländerzentralregister, or AZR for short), a database that contains personal information on about 20 million foreign nationals, into a shared repository for certain master data, such as names and fingerprints. However, this transformation did not include workflow management features.

Moreover, the transformation revealed three challenges for creating a centralized solution for the German asylum procedure. First, centralization requires the redistribution of competencies, which, in turn, requires considerable legislative action. In particular, the existence of the AZR requires a specific AZR law. While this law provides a solid legal foundation, it also reduces the AZR's flexibility, as technical

updates first require Germany's parliament to make a formal legislative update to the AZR law. Second, centralization creates unbalanced data guardianship arrangements. In particular, the BAMF has to assume full responsibility for the lawfulness of the subsequent processing of any data in the AZR. Third, centralization leads to the development of solutions that do not take account of the specifics of individual workflows. In particular, the AZR's data model includes only a fraction of the data typically exchanged between authorities over the course of the workflow involved in processing asylum applications.

Identifying Blockchain as a Potential Solution for the Asylum Procedure

These shortcomings encouraged the BAMF to explore decentralized alternatives for cross-organizational workflow coordination, which would require neither the delegation of workflow governance to a single authority nor the extension of the AZR. After a preliminary evaluation, the BAMF narrowed down its technological options and decided to consider a blockchain solution. This choice was based on best practices for the identification of blockchain use cases and essentially followed the first seven questions of the ten-step decision path described by Pedersen et al.[21]

The solution the BAMF sought was a shared common database for event logs (Question 1 in the ten-step path) that would be used by multiple parties (Question 2). Although trust is not necessarily an issue between the authorities involved in the German asylum procedure, the federal nature of the process means that it incorporates a multitude of interests that are often not fully aligned (Question 3). Concerns about competencies, data guardianship, and flexibility caused the BAMF to seek a decentralized solution (Question 4). Moreover, it argued that a solution for cross-organizational workflow coordination would have to offer tiered rights of access because most authorities involved in the procedure are only entitled to view specific data (Question 5). The rules of the procedure, meanwhile, would remain predominately the same (Question 6), and the BAMF was interested in creating an immutable log that would facilitate process forensics at a later point (Question 7).

Choosing the Blockchain Design

Access right considerations caused the BAMF to choose a private permissioned blockchain design. Blockchain networks are deemed "private" when reading access is limited to a certain set of participants, such as the authorities involved in the asylum procedure, whereas a public blockchain network allows anyone to read transactions. "Permissioned" means that only preregistered participants can submit new transactions, validate those transactions, and append new blocks; in a permissionless network, any participant can do so.[22] The BAMF chose to make its blockchain solution permissioned because the authorities in the asylum procedure are known and have clearly designated roles and competencies.

A private permissioned blockchain solution offered the BAMF several functional and technical benefits over the status quo. Functionally, such a solution would improve integrity and increase the speed of procedures. Lengthy asylum procedures regularly result in undue hardship for applicants, negative press coverage, and protracted revisions in court. The BAMF was particularly interested in blockchain technology's ability to use event logs to quickly establish a shared truth on the status and course of asylum applications, as illustrated by the manager of the BAMF's blockchain project:

> *"Blockchain is a promising technology that can support communication and collaboration among the public authorities involved in asylum procedures. It offers many advantages, especially for sharing status updates quickly and securely: the authorities involved can obtain an overview of the course of an applicant's asylum procedure via the blockchain and can call up the status almost in real time."* Haris Trtovac, Manager of the BAMF's blockchain project

Technically, a blockchain solution could provide the BAMF with flexibility, which would

21 Pedersen, A. B., Risius, M., and Beck, R. "A Ten-Step Decision Path to Determine When to Use Blockchain Technologies," *MIS Quarterly Executive* (18:2), June, 2019, pp. 99-115. This article provides a comprehensive discussion of what constitutes a genuine blockchain use case.

22 For detailed information on the differences between these blockchain design choices, see Androulaki, E. et al. "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," *Proceedings of the Thirteenth EuroSys Conference*, April 23-26, 2018, ACM Digital Library, available at https://dl.acm.org/citation.cfm?id=3190538.

only require agreement on data models and application programming interfaces (APIs). Moreover, it recognized blockchain's potential to further the once-only principle:[23]

> *"In the future, we should no longer copy data into large nationwide databases. Rather, we should leave the data where we collect it and use a logging layer to make transparent when and where status changes occurred. With a lightweight blockchain solution, we can more easily implement this logging layer than with an expansion of the existing and already complex IT solutions."* Markus Richter, Vice President of the BAMF

How the BAMF Ensured its Blockchain Solution Is GDPR-compliant

Proof-of-Concept and Pilot Stages

The BAMF began its blockchain project in January 2018 with a proof of concept intended to demonstrate that a blockchain solution could offer the functionality required to coordinate the workflow underlying the German asylum procedure. The prototype used a blockchain to log and propagate the completion of essential steps in the procedure. It matched these event logs to asylum applications using AZR identification numbers.

Although the prototype was successful in demonstrating blockchain technology's functional merits, the BAMF was concerned about compliance with the GDPR, which took effect in May 2018. The BAMF therefore commissioned a legal opinion,[24] which raised serious concerns about the prototype's data model. In particular, the opinion argued that, while the event logs did not themselves qualify as personal data, the use of the AZR identifiers turned each event log into personal data, which would eventually have to be erased. The opinion urged the BAMF to address three issues:

1. Define the responsibilities for compliance with the requirements of the GDPR
2. Establish the lawful bases for processing personal data
3. Create a design that would allow personal data to be rectified and erased. Ideally, the design would either use a so-called redactable blockchain or pseudonymize the personal data.

The BAMF addressed these issues during the subsequent pilot phase. To limit complexity, the BAMF decided to focus on the Saxony Arrival, Decision, and Return (AnkER) facility, which opened in Dresden mid-2018. (The aim is for the initial processing of all asylum seekers to take place in AnkER facilities.) To improve information exchange and expedite procedures, several authorities are involved in the AnkER procedure. The BAMF approached Saxony's central immigration authority (the LDS), with the aim of jointly creating and testing a blockchain solution for coordinating those parts of the AnkER procedure that required the closest collaboration between the BAMF and the LDS.

To mitigate the lack of best practices for managing the requirements of the GDPR and developing a GDPR-compliant solution, the BAMF held several idea-generation workshops and architectural refinement meetings. The BAMF also met with Germany's Federal Commissioner for Data Protection and Freedom of Information (BfDI). In two workshops, the BAMF and experts from the BfDI discussed the prototype and the BAMF's propositions for a GDPR-compliant solution.

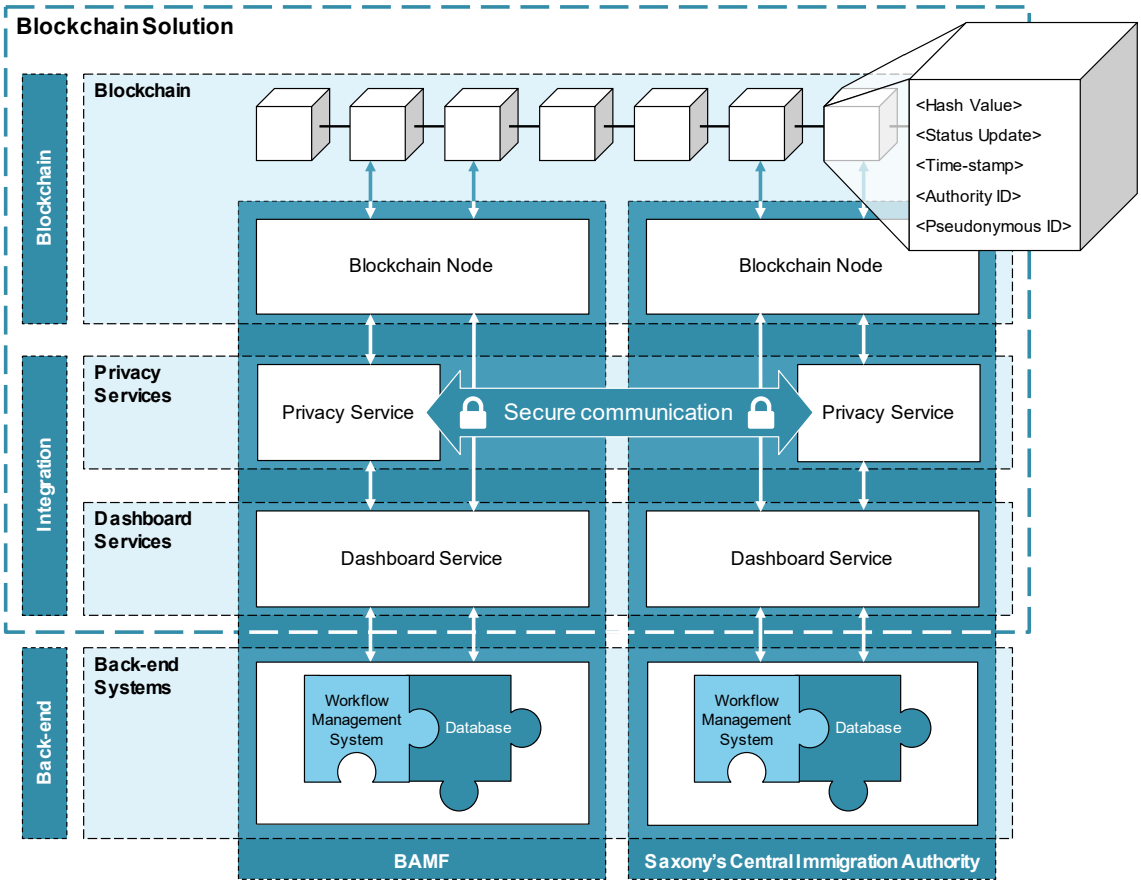
Choosing the Blockchain Solution Approach

Because it wanted to avoid the creation of a central authority, the BAMF used the pseudonymization approach to ensure that its blockchain solution is GDPR-compliant. It also determined that encryption and hashing were impractical choices for the pseudonymization

23 The European Commission's *Communication on the eGovernment Action Plan 2016 – 2020* sets out several principles, including the "once only principle," which states that "public administrations should ensure that citizens and businesses supply the same information only once to a public administration. Public administration offices take action if permitted to internally reuse this data, in due respect of data protection rules, so that no additional burden falls on citizens and businesses.", available at https://ec.europa.eu/digital-single-market/en/news/communication-eu-egovernment-action-plan-2016-2020-accelerating-digital-transformation

24 For the full opinion (in German only), see Hoeren, T. and Baur, J. *Datenschutzrechtliche Zulässigkeit der Übermittlung von Informationen über Migranten zwischen öffentlichen Stellen mittels einer Permissioned-Biockchain,* 2018, available at https://fragdenstaat.de/anfrage/gutachten-blockchainbamf/302470/anhang/ifg_gutachten_blockchain.pdf.

Figure 1: Three-Level Architecture of the BAMF's Blockchain Solution



of event logs on the blockchain. It rejected encryption because this would limit the network's ability to validate transactions and because managing and distributing individual encryption keys for each event log would create substantial complexity. Encryption with static keys might eventually lead to all participants being able to decrypt all event logs, which would, in turn, make all participants joint controllers. It chose not to use cryptographic hash functions because this would reduce the blockchain to a simple notarization[25] solution with very limited options for the use of smart contracts. Moreover, such a solution would require the redundant exchange of event logs via another channel.

Instead, the BAMF decided to implement a pseudonymous identifier solution with so-called privacy services. With this solution, each participant operates an off-chain service that maps pseudonymous identifiers on the blockchain to the IDs used by the participant, and does so in a privacy-compliant, erasable, and rectifiable manner. Without the mapping, the BAMF (and other authorities involved in the blockchain solution) cannot attribute the data on the blockchain to a natural person. In order to enable the sharing of meaningful information, privacy services can exchange mapping information through secure communication channels.

Creation of a Joint Control Arrangement

Through an administrative agreement, the BAMF created a joint control arrangement with the LDS that established the purpose and means of processing and assigned responsibilities for GDPR compliance. In terms of purpose and

25 According to the National Notary Association, "Notarization is the official fraud-deterrent process that assures the parties of a transaction that a document is authentic, and can be trusted." For more information, see https://www.nationalnotary.org/knowledge-center/about-notaries/what-is-notarization.

means, the agreement specified the storage and exchange of event logs required for collaborating, via the blockchain solution throughout the AnkER procedure. In terms of responsibilities, the agreement specified that the BAMF would host and assume responsibility for the data stored on the blockchain and for the privacy services. However, for each event log submitted to the blockchain, such as the BAMF's ruling on an asylum application, the LDS and the BAMF would have to independently verify whether they have a lawful basis for submission; once the event log is written to the blockchain, the other authority is responsible for establishing its own lawful basis before reading the log. For each piece of mapping information exchanged between the privacy services, the sending authority must verify that it has a lawful basis for sending, and the receiving authority must to establish whether it has a lawful basis for adding the information to its mapping database. To minimize complexity, the BAMF and the LDS consulted the relevant legislation to establish up-front the required lawful bases for each conceivable type of data exchange.

The BAMF's Blockchain Solution Architecture

In terms of technical measures, the BAMF implemented a blockchain architecture with three layers (see Figure 1). Layer 1 (back-end systems) holds the existing workflow management systems and data repositories of the authorities involved. The other two layers do not need to be integrated with these back-end systems; instead, they can be loosely coupled through a set of APIs. Layer 2 (integration) hosts dashboard services, which create the event logs and can display to users data from both the back-end systems and the blockchain (Layer 3). Layer 2 also hosts privacy services, which map the pseudonymous blockchain IDs with the specific IDs used in the back-end systems. The design of Layers 1 and 2 can vary between the authorities involved in the blockchain solution; only the blockchain layer is standardized across all authorities.

Blockchain Layer. The blockchain layer propagates pseudonymized event logs, with each entry consisting of four elements—a status update, a time-stamp, the ID of the authority that created the status update and a pseudonymous ID. From a functional perspective, these elements reflect the minimum amount of data required for effective use. From a GDPR perspective, they are sufficiently nonspecific to limit the risk of inadvertent attribution—for example, through the analysis of the trail of event logs.[26]

Integration Layer—Privacy Services. In order to attribute the event logs on the blockchain, the BAMF created a network of authority-specific privacy services, with each authority hosting a standalone privacy service. Each service contains databases that map the pseudonymous IDs to the specific IDs—such as application or personal identification numbers—used in the authority's back-end systems. The privacy services support role-based access procedures for different user groups within authorities, and can exchange mapping information. Such an exchange is important for the handover of an asylum application to another authority.[27] Moreover, the services can exchange requests for the erasure of mappings related to a pseudonymous ID.

Integration Layer—Dashboard Services. In order to submit event logs to the blockchain and display data from both the blockchain and the back-end systems, the BAMF implemented dashboard services. Event logs can be submitted manually to the dashboard services, or by drawing (pull-based mechanism) or receiving (push-based mechanism) the data from the back-end systems. The dashboard services then convert the event log data to comply with the blockchain's data model. To display the data, users access the dashboard services through a web browser and enter various commands, such as "display the history of a certain procedure" or "display all procedures that meet certain conditions. The dashboard will then, in accordance with the access rights of the user and the mapping information in the privacy service, collect and display attributed event logs from the

26 The risk of inadvertent attribution from spatiotemporal data—i.e., data points with both location and time attributes—is high because the four data points can be sufficient to uniquely identify a person (linkability risk). For a detailed discussion of the linkability risk of anonymized mobility data, see de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M. and Blondel, V. D. "Unique in the Crowd: The privacy bounds of human mobility," *Scientific Reports* (3), March 2013, Article 1376.

27 From a legal perspective, every such exchange equates to the processing of personal data, and requires both the sending and receiving authority to establish a lawful basis.

blockchain layer and further information from the back-end systems of the authority. Importantly, a user can only view information for which the authority and the user have clearance and a lawful basis.

Ensuring Privacy by Design

Erasure by Design. Erasure of personal data from a blockchain may become necessary for several reasons, such as simple errors in entering data, or the expiration of a lawful basis. Explicit time limits in the German Asylum Act, for instance, ensure that authorities do not store personal data for more than a maximum of ten years after the completion of a procedure.

The erasure procedure implemented in the BAMF's blockchain solution is triggered by an authority issuing a command to its privacy service, which deletes the respective mapping and submits a so-called "erasure event log" to the blockchain. An erasure event log on the blockchain invalidates the pseudonymous blockchain ID and prevents further use of this ID by all authorities in the blockchain network. Moreover, the log informs other authorities of the erasure. Each joint controller who receives this information can then use the erasure event log as a trigger to re examine all the lawful bases. For those events for which the joint controllers still have a lawful basis, they can create and submit copies to the blockchain under a new pseudonymous ID.

Conceptually, the erasure procedure could also be useful for off-chain information exchange related to an event log. Currently, authorities check whether data requests from other authorities are legitimate, but often do not keep a record of these requests or the data they forward. This means that authorities are unable to direct requests for erasure and rectification to specific authorities. The blockchain solution, however, would ensure that such requests for erasure reach all authorities in the blockchain network.

Rectification by Design. In addition to the erasure procedure, the BAMF also implemented a rectification procedure. Rectification may become necessary if, for example, false event logs are submitted to the blockchain or duplicate blockchain IDs need to be reconciled. The rectification procedure mirrors the erasure procedure and is triggered by specific rectification actions in the back-end systems. Rectification actions are submitted to the blockchain as "rectification events." Other authorities can respond to rectification events by, for instance, approaching the issuing authority for further information, and/or stopping or reversing subsequent steps in the asylum procedure. If there are duplicates, the privacy service adjusts its mapping and retires one of the duplicate blockchain IDs.

Recommendations for Ensuring Blockchain Solutions Are GDPR-Compliant

We distilled three key learnings from the BAMF project and have translated these into three recommendations. These recommendations should be interpreted as high-level guidelines rather than as a reference architecture or legal advice. In line with the European parliament,[28] we advise each blockchain project to seek its own legal assessment and to design its own portfolio of organizational and technical measures.

1. Avoid Storing Personal Data on a Blockchain

Blockchain solutions should be designed so that it is not necessary to store personal data on the blockchain. Instead, personal data should remain in systems that permit rectification and erasure. This advice also applies to any attribute on a blockchain that allows identification of an individual by analyzing patterns of use or context.

2. A Blockchain Solution that Needs to Process Personal Data Should Use a Private and Permissioned Pseudonymization Approach

If a blockchain solution will process personal data, we recommend using the pseudonymization approach, because a central authority or shared responsibility approach will be impractical in most instances. Moreover, a pseudonymization approach simplifies the identification of controllers. All those who hold the additional information required for attribution qualify as

28 "Compatibility between distributed ledgers and the GDPR can only be assessed on the basis of a detailed case-by-case analysis that accounts for the specific technical design and governance set-up of the relevant blockchain use case." European Parliament, 2019.

(joint) controllers unless otherwise specified in an agreement for processing personal data.

When the solution requires two or more participants to share additional information for attribution, we strongly recommend establishing a private and permissioned blockchain network. This will simplify the establishment and management of arrangements required for joint control or agreements for processing personal data. In particular, a private network enables the establishment of a controlled introduction process during which new participants can be added to the arrangements or agreements. A permissioned network facilitates the creation of a flexible and role-based model for the allocation of responsibilities.

To avoid inadvertent attribution, however, even pseudonymized data should be limited to an absolute minimum. Moreover, the solution should store information required for attribution in a highly secure manner, as any uncontrolled disclosure may require the blockchain to be modified.

3. A Blockchain Solution that Needs to Coordinate Cross-Organizational Workflows Should Use a Private and Permissioned Pseudonymization Approach with Identifier Mapping

For cross-organizational workflows, the pseudonymization approach with identifier mapping—i.e., separate mapping databases for each participant—provides the best trade-off between value and security. Although storing only hashed event logs on the blockchain would be more secure, this approach would require the redundant exchange of the unhashed data and would limit the use of the blockchain solution to simple notarization. Storing encrypted event logs on the blockchain would be just as useful as identifier mapping but would require each event log to be encrypted with a separate encryption key, which would significantly increase the complexity and vulnerability of the overall blockchain solution.

Concluding Remarks

"GDPR compliance is not about the technology, it is about how the technology is used. Just like there is no GDPR-compliant Internet or GDPR-compliant artificial intelligence algorithm, there is no such thing as a GDPR-compliant blockchain technology. There are only GDPR-compliant use cases and applications."[29]

The BAMF has created a GDPR-compliant blockchain application through a combination of organizational and technical measures. The BAMF application for processing asylum applications thus demonstrates that blockchain technology and the GDPR are not incompatible and suggests that organizations should continue to explore and develop blockchain solutions that will involve the processing of personal data. Because blockchain solutions emphasize decentralized governance, they could be a particularly promising alternative in cross-organizational settings that prevent the delegation of workflow governance to a central authority. A next essential step for the widespread deployment of GDPR-compliant blockchain applications will be to establish standards and reference architectures that ensure the interoperability of various blockchain technologies and solutions.

Appendix A: The German Asylum Procedure

The German Constitution grants anyone persecuted on political grounds the right to asylum. This right also extends to those fleeing from violence, war, or terrorism.

29 Lyons, T., Courcelas, L. and Timsit, K., op. cit., October 16, 2018.

Figure 2: Steps in the German Asylum Procedure

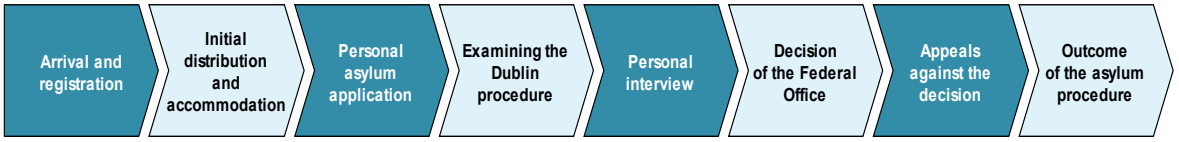


Table 2: BAMF Blockchain Team Members Interviewed

Role in the Blockchain Project	Focus
Director of the AnkER and functional project lead with more than 15 years' experience	Functional benefits, design principles, and data privacy
Business process manager with more than 15 years' experience	Functional benefits, design principles, and data privacy
Lawyer, GDPR compliance-responsible team member with more than 15 years' experience	Data privacy
Lawyer, GDPR compliance-responsible team member with more than 15 years' experience	Functional benefits, design principles, and data privacy
Project manager with more than 20 years' experience, responsible for communication with the c-suite	Functional benefits, design principle, and data privacy

Figure 2 shows a simplified version of the German asylum procedure. On arriving in Germany, federal law requires asylum seekers to immediately report to federal or state police and make a request for asylum. The police will then take them to the closest registration agency, where they will have access to medical care, and the registration agency provides them with a proof-of-arrival document that grants a temporary right to stay. While at the registration agency, asylum seekers can also register their application with the BAMF. The BAMF checks if another member state of the European Union has previously registered the applicant. If that check is positive, the Dublin Regulation stipulates that the refugee must be returned to the member

Table 3: External Blockchain Experts Interviewed

Interviewee	Experience	Focus
Serial blockchain entrepreneur	Founder and CEO of a blockchain startup that has implemented a blockchain-based payment system in the refugee context	Functional benefits, design principles, and principles for blockchain decision paths
Blockchain consultant	Blockchain consultant who has worked since 2015 for T-Systems MMS, and has been involved with multiple blockchain proofs of concept and pilots	Functional benefits, design principles, and principles for blockchain decision paths
Blockchain researcher and consultant	Blockchain researcher and solution architect who has worked since 2018 for Centrifuge, which provides an open, decentralized operating system that aims to connect the global financial supply chain	Functional benefits, design principles, and impact of blockchain on IT strategies
Blockchain researcher and consultant	Associate partner who has worked since 2008 for a Fortune 500 technology company closely involved with Hyperledger Fabric	Functional benefits, design principles, and data privacy
Blockchain developer	Blockchain developer and solution architect who has worked since 2016 for the NEM Foundation, which provides technical support for the NEM ecosystems	Functional benefits, design principles, and data privacy
Blockchain researcher and consultant	Founder and CEO of a blockchain startup founded in 2016 to provide secure and GDPR-compliant data exchange	Functional benefits, design principles, and data privacy
Blockchain researcher and consultant	Junior IT manager who has worked since 2017 for a globally active automotive supplier on technology research and implementation	Functional benefits, design principles, and data privacy
Blockchain developer	Blockchain developer and solution architect who has worked since 2016 for a globally active automotive supplier	Functional benefits, design principles, and data privacy
Blockchain entrepreneur	Co-founder of a blockchain startup that offers digital infrastructure services for innovative electricity tariffs	Functional benefits, design principles, and data privacy
Blockchain researcher and consultant	Blockchain Ph.D. student and consultant who has worked since 2014 for one of the largest research institutions in Europe	Functional benefits, design principles, and data privacy

state in which he or she was first registered. This check, however, can take up to several days. Meanwhile, refugees may have to relocate to a different registration agency based on their nationality and Germany's federal quota system.

If the check is negative, the BAMF will hold a personal interview at the closest appropriate registration agency or a regional office. A BAMF caseworker will then decide whether to approve or reject the application for asylum. The caseworker justifies the decision in a written document that is given to the applicant. If the caseworker rejects the application, the applicant can appeal the decision in court. Favorable decisions result in the applicant being granted a residence permit. If the application is rejected, the relevant immigration authority repatriates the applicant. More details on the German asylum procedure are available in the BAMF's overview document.[30]

Appendix B: Research Method

There is a dearth of detailed accounts of and knowledge about developing GDPR-compliant blockchain applications. In the public sector, in particular, most governmental agencies remain unfamiliar with blockchain technology. Our research thus required us to provide substantial guidance to the BAMF on developing its blockchain solution, as well as to other agencies, such as the Federal Commissioner for Data Protection and Freedom of Information, to help them assess the solution's GDPR-compliance.

As a consequence, we chose an action research[31] approach, with three of our co-authors providing advisory services to the BAMF's blockchain project from January 2018 onward. These three co-authors familiarized the BAMF team with blockchain technology and organized an ongoing cycle of cross-team reflections, which continued throughout the project.[32] One co-author, for instance, worked closely with the IT vendor hired by the BAMF to implement the blockchain solution and guided the BAMF's architectural board. Two other co-authors were not involved with the project team's operations but acted as external observers. The combination of three collaborating and two observing researchers allowed us to maintain high standards of evidence gathering and academic rigor.

In the course of the project, we gathered evidence from four different sources:

1. We held various workshops on functional, technical, and data privacy issues
2. We regularly participated in and contributed to developer meetings and architectural reviews
3. We analyzed public blockchain interviews of BAMF employees and conducted 15 additional semistructured interviews with blockchain project team members and blockchain experts. These interviews lasted between 40 minutes and two hours and each was recorded
4. We reviewed and analyzed various internal and external documents on the blockchain project.

Blockchain Workshops and Contribution to Technical Meetings

During the project, the three collaborating co-authors held nearly 30 blockchain workshops. The range of attendees included BAMF employees, employees of Saxony's central immigration authority (the LDS), employees of the Federal and the Saxony Ministries of the Interior, a delegation from the Federal Commissioner for Data Protection and Freedom of Information, employees of the Dutch Immigration and Naturalization Service, and several other organizations. In these workshops, we focused on various functional, technological and data privacy issues. To deliver the educational segments of these workshops,

30 *The stages of the German Asylum Procedure: An Overview of the Individual Procedural Steps and the Legal Basis*, 2016, Federal Office for Migration and Refugees, available at http://www.bamf.de/SharedDocs/Anlagen/EN/Publikationen/Broschueren/das-deutsche-asylverfahren.pdf?__blob=publicationFile.

31 Action research emphasizes (participatory) observation in the field to address a specific problem (in this case, enabling digital federalism through a GDPR-compliant blockchain architecture). For more information on action research, see Baskerville, R. and Myers, M. D. "Special Issue: Action Research in Information Systems," *MIS Quarterly* (28:3), September 2004, pp. 329-335.

32 Avison, D., Baskerville, R., Myers, M. and Wood-Harper, T. "IS action research: can we serve two masters? (panel session)," Kock, N., panel chairman, *Proceedings of the 20th International Conference on Information Systems*, December 1999, pp. 582-585.

Table 4: BAMF Employees Public Blockchain Interviews Analyzed

Public Interview Reported in:	Interviewee and Position	Focus
Behörden Spiegel	Dr. Markus Richter (BAMF CIO from Jan 2018 – July 2018 and BAMF vice president since July 2018)	Functional and technical benefits and data privacy
Der Spiegel	Dr. Markus Richter (BAMF CIO from Jan 2018 – July 2018 and BAMF vice president since July 2018)	Functional and technical benefits and data privacy
Bundesamt für Migration und Flüchtlinge – Digitalisierungsagenda 2020	Haris Trtovac (BAMF blockchain project manager since April 2018)	Functional and technical benefits and data privacy
Bundesamt fürMigration und Flüchtlinge – Digitalisierungsagenda 2020	Kausik Munsi (BAMF CTO)	Functional and technical benefits, data privacy and impact of blockchain on the BAMF's IT strategy

we adapted the method of Fridgen et al.[33] In the conceptual segments, we used creative elements to access the attendees' prior experiences and knowledge and to further their involvement.

In addition to these workshops, we collaborated with the BAMF team members on a daily basis in stand-up meetings, development meetings, and management calls. We were routinely involved in architectural as well as sprint review and planning meetings. In particular, we suggested multiple refinements to the blockchain solution and helped resolve technical and data-privacy issues. For instance, we developed the erasure and rectification concepts and contributed essential elements to the privacy service concept.

Interviews with BAMF Stakeholders, Team Members, and Experts

Given the novelty of blockchain technology and the related challenges, we complemented our action research approach by conducting interviews, which are a preferred method for extracting explorative knowledge. In total, we conducted 15 interviews, five with project team members and 10 with various blockchain experts. We used an interview guide for these semistructured interviews, which allowed the interviews to flow naturally but also ensured comparability between the interviews. An open dialogue, rather than the rigorous use of predefined questions, helped to maximize the depth of insights provided by interviewees, who thus delivered valuable knowledge that supported the subsequent development of the recommendations.[34]

Because all blockchain team members preferred to remain anonymous, the table below provides only anonymized information on their roles in the blockchain project and their prior experience.

We also conducted ten semistructured interviews with external blockchain experts (as listed in the next table), some of whom preferred to remain anonymous.

In addition, we analyzed public blockchain interviews given by four BAMF employees, listed in Table 4.

Analysis of Internal and Public Documents

We also analyzed several hundred pages of BAMF internal memos, reports, analyses, and meeting minutes. Importantly, these internal documents included highly relevant strategy papers, data privacy analyses, and architectural specifications. We also reviewed the BAMF's public documents, such as its digitalization

33 Fridgen, G., Lockl, J., Radszuwill, S., Rieger, A., Schweizer, A. and Urbach, N. "A Solution in Search of a Problem: A Method for the Development of Blockchain Use Cases," *Proceedings of the Americas Conference on Information Systems*, August 2018, pp. 1-10.

34 Urquhart, C., Lehmann, H. and Myers, M. D. "Putting the 'theory' back into grounded theory: guidelines for grounded theory studies in information systems," *Information Systems Journal* (20:4), July 2010, pp. 357-381.

agenda and blockchain webpage. Lastly, but importantly, we reviewed legal analyses and the data privacy advice issued by lawyers and renowned German scholars concerning blockchain, legal decisions in comparable scenarios, and governmental papers on comparable blockchain use cases.

Analyzing the Evidence from the Sources

To analyze the evidence, we first consolidated our sources of data and the data itself to eliminate redundancies. Next, we clarified imprecise statements and added—where needed—explanatory comments to data points. Third, we assigned codes to the data points and developed tentative principles through open and, later, axial coding. Where the data related to new phenomena, we marked the passages and discussed them within the research team, building new principles when necessary.[35] We iteratively adapted the codes until they were collectively exhaustive and mutually exclusive. Subsequently, we discussed the resultant principles with the practitioners in order to gain other perspectives.

About the Authors

Alexander Rieger

Alexander Rieger (alexander.rieger@fim-rc.de) is a doctoral candidate at the Finance & Information Management (FIM) Research Center and the Project Group Business & Information Systems Engineering of the Fraunhofer FIT, University of Augsburg. His professional interests include innovative digital technologies such as blockchain and artificial intelligence, and, more specifically, their strategic implications and adoption. Prior to joining the BAMF's blockchain project in February 2018, Alex spent several years working in industry and consulting.

Florian Guggenmos

Florian Guggenmos (florian.guggenmos@fim-rc.de) is a doctoral candidate at the Finance & Information Management (FIM) Research Center and the Project Group Business & Information Systems Engineering of the Fraunhofer FIT, University of Bayreuth. His current research focuses on systemic risk management as well as data privacy and information security, particularly in the context of digitalization projects. Florian has also worked on a range of applied research projects. He joined the BAMF's blockchain project in February 2018.

Jannik Lockl

Jannik Lockl (jannik.lockl@fim-rc.de) is a doctoral candidate at the Finance & Information Management (FIM) Research Center and the Project Group Business & Information Systems Engineering of the Fraunhofer FIT, University of Bayreuth. His main focus is on the Internet of Things (IoT) as well as the wider adoption of digital technologies and the socioeconomic embedding of blockchain applications. Jannik worked as a consultant on a variety of industry projects before joining the BAMF's blockchain project in February 2018.

Gilbert Fridgen

Gilbert Fridgen (gilbert.fridgen@uni.lu) is PayPal-FNR PEARL Chair in Digital Financial Services in the Interdisciplinary Center for Security, Reliability and Trust (SnT) at the University of Luxembourg. His work focuses on smart grids, the machine economy, and blockchain technology in both the public and private sectors. Gilbert's work has been published in several prominent IS, management, computer science and engineering journals. He has also managed various industry research projects and received multiple research grants. Gilbert has served as expert counsel to many German government bodies, including the Bundestag and six German federal ministries, and also to the European Commission through its European Blockchain Partnership.

Nils Urbach

Nils Urbach (nils.urbach@fim-rc.de) is a professor of information systems and strategic IT Management at the University of Bayreuth. He is deputy director of the Finance & Information Management (FIM) Research Center and of the Project Group Business & Information Systems Engineering of Fraunhofer FIT. He is also a co-founder and director of the Fraunhofer BlockchainLab. Nils' research focuses on digital transformation, blockchain, and the management of artificial intelligence. His work has been published in leading journals including *MIS*

35 Strauss, A. and Corbin, J. M. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques,* 1990, Sage Publications.

Quarterly Executive, Journal of Information Technology, and *The Journal of Strategic Information Systems*. Before his academic career, Nils worked for several years as a management consultant.