MIS Quarterly Executive

Volume 24 | Issue 1 Article 8

March 2025

How Germany Successfully Implemented Its Intergovernmental FLORA System

Julia Amend

Simon Feulner

Alexander Rieger

Tamara Roth

Gilbert Fridgen

See next page for additional authors

How Germany Successfully Implemented Its Intergovernmental FLORA System

Authors
Julia Amend, Simon Feulner, Alexander Rieger, Tamara Roth, Gilbert Fridgen, and Tobias Guggenberger

MIS QUARTERLY EXECUTIVE

How Germany Successfully Implemented Its Intergovernmental FLORA System

Developing and deploying intergovernmental IT systems across layers of government (e.g., state and federal) is challenging because the law requires cooperation but also mandates that each layer has its own separate IT systems. We describe how Germany successfully navigated the challenges when it implemented FLORA, a blockchain-based system that supports the processing of asylum seekers. Based on insights gained from FLORA, we provide three recommendations for successfully implementing intergovernmental IT systems.[1,2]

Julia Amend
FIM Research Center, Branch Business & Information Systems Engineering of Fraunhofer FIT, University of Bayreuth (Germany)

Simon Feulner
FIM Research Center, Branch Business & Information Systems Engineering of Fraunhofer FIT, University of Bayreuth and Frankfurt University of Applied Sciences (Germany)

Alexander Rieger
University of Arkansas (U.S.)

Tamara Roth
University of Arkansas (U.S.) and University of Luxembourg (Luxembourg)

Gilbert Fridgen
University of Luxembourg (Luxembourg)

Tobias Guggenberger
FIM Research Center, Branch Business & Information Systems Engineering of Fraunhofer FIT and University of Bayreuth (Germany)

Building Intergovernmental IT Systems Is Challenging

Governments are investing significant effort and resources to move their services into the digital age.[3] The U.S. Federal Government, for instance, had an IT budget of $98.1 billion in

[1] Mary Lacity is the senior accepting editor for this article.

[2] We would like to express our gratitude to Mary Lacity and the two anonymous reviewers for their guidance and comments, which considerably improved this article. Our research was funded in part by the Luxembourg National Research Fund (FNR) and PayPal, PEARL (grant reference 13342933/Gilbert Fridgen). For the purpose of open access, and in fulfillment of the obligations arising from the grant agreement, Gilbert Fridgen has applied a Creative Commons Attribution 4.0 International (CC BY 4.0) license to any author-accepted manuscript version arising from this article.

[3] See for, example: 1) Bui, Q. N. "Increasing the Relevance of Enterprise Architecture through "Crisitunities" in U.S. State Governments," *MIS Quarterly Executive* (14:4), December 2015, pp. 169-179; and 2) Kim, S. L. and Teo, T. "Lessons for Software Development Ecosystems: South Korea's e-Government Open Source Initiative," *MIS Quarterly Executive* (12:2), June 2013, pp. 93-108.

DOI: 10.17705/2msqe.00112

2024, of which $29.1 billion was earmarked for major investments.[4] However, these investments can be difficult to translate into secure and efficient services. Many government services require that multiple levels of government cooperate, but their competencies, budgets and—by extension—IT systems are legally separated. This separation often results in complex and multilayered IT architectures that complicate information exchange and are difficult to modernize. Cooperation between federal and state governments is a prime example. The two levels have distinct competencies, and each state has its own budgets and IT systems. Introducing new IT systems to support cooperation between different levels of government is therefore challenging.[5]

Despite the challenges, government levels can bridge the divide. In this article, we describe one such example from Germany, where the federal and state governments introduced FLORA, a system for coordinating the processing of asylum applications (referred to in Germany, and throughout this article, as the "asylum procedure").

Overview of Germany's Asylum Procedure and the FLORA System

In 2024, Germany processed around 352,000 asylum applications.[6] Its asylum procedure is federally organized and requires various agencies to closely cooperate. The Federal Office for Migration and Refugees is at the core of the procedure and manages and issues decisions on asylum applications. It collaborates closely with migration agencies in Germany's 16 states, which are responsible for the initial registration of asylum seekers, and their eventual integration or repatriation. Also involved are health agencies that provide medical care, translation service providers that support interviews, educational service providers that offer language courses, and law enforcement agencies that complete background checks and facilitate repatriations. Figure 1 depicts the initial stages of the asylum procedure, highlighting its complexity.[7]

All involved agencies (and partner organizations) are subject to a tight legal framework that defines the distribution of responsibilities and rules for the asylum procedure. This framework also mandates that most of the agencies have their own processes and IT systems. The resulting fragmentation of IT systems complicates collaboration and the exchange of asylum procedure information across agency and system boundaries. Prior to FLORA, most asylum cases involved Excel-based lists that were manually filled and exchanged via email, which took a lot of time and was very error-prone.

FLORA's introduction to support the initial stages of the asylum procedure (up to the personal interview) eliminated most Excel-based lists and streamlined the exchange of procedural information. Moreover, FLORA improved the quality of information, reduced the time required by up to 50%, and minimized the risks of errors and data privacy violations.[8]

FLORA is a particularly rich case study because its development was fraught with many of the challenges that too often weigh down intergovernmental IT systems. First, we explain how the implementation of FLORA overcame these challenges. We then describe FLORA's private permissioned blockchain architecture and the governance of the system. Finally, based on insights gained from the FLORA case, we provide three recommendations for building intergovernmental IT systems that can bring multilevel government services into the digital age.

[4] For information on the United States' federal IT spending, see *The Federal IT Dashboard, General Services Administration*, available at https://itdashboard.gov/.

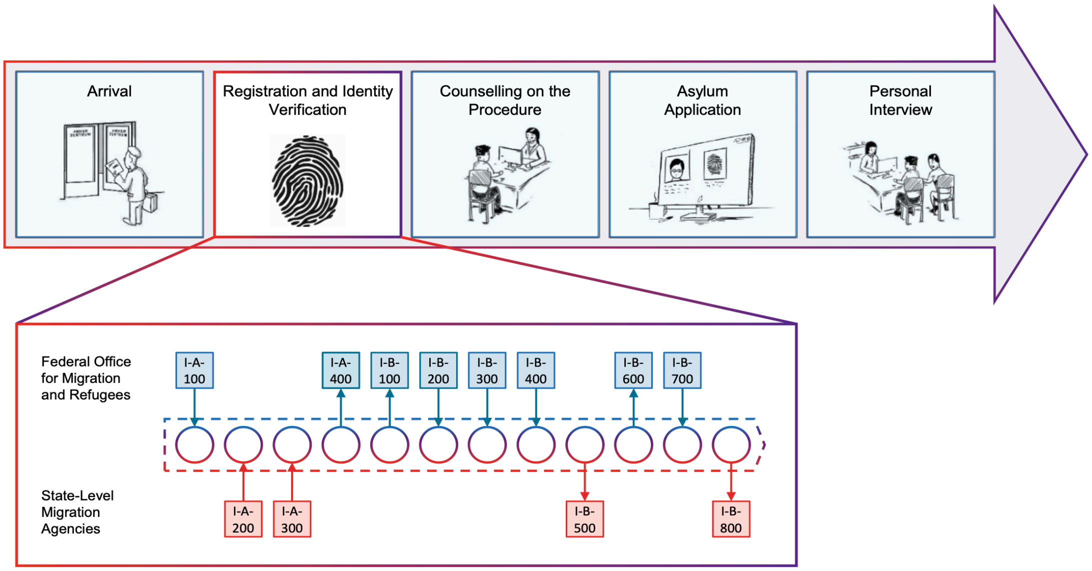
[5] Insights into the challenges of government IT projects can be found in: Pahlka, J. *Recoding America: Why Government is Failing in the Digital Age and How We Can Do Better*, Metropolitan Books, 2023.

[6] For more details, see *Asylum Figures for the Entire Year and December 2024*, Federal Office for Migration and Refugees, January 2025, available at https://www.bamf.de/SharedDocs/Meldungen/DE/2025/250109-asylzahlen-dezember-und-gesamtjahr-2024.html?nn=282600.

[7] For a description of the procedure, see *The Stages of the Asylum Procedure*, Federal Office for Migration and Refugees, available at https://www.bamf.de/EN/Themen/AsylFluechtlingsschutz/AblaufAsylverfahrens/ablaufasylverfahrens-node.html

[8] For details on data processing in Germany's asylum procedure, see: https://www.bamf.de/SharedDocs/Anlagen/EN/EMN/Studien/wp90-datenmanagement.pdf?__blob=publicationFile&v=1.

Figure 1: Initial Stages of Germany's Asylum Procedure


Arrival
Registration and Identity Verification
Counselling on the Procedure
Asylum Application
Personal Interview
Federal Office for Migration and Refugees
I-A-100
I-A-400
I-B-100
I-B-200
I-B-300
I-B-400
I-B-600
I-B-700
State-Level Migration Agencies
I-A-200
I-A-300
I-B-500
I-B-800

Development and Deployment of FLORA

In response to the European refugee crisis in 2015/2016, the Federal Office for Migration and Refugees substantially increased its investments in digital technologies that would make the asylum procedure more efficient, secure and scalable. These technologies included advanced validation tools, such as facial recognition to complement the validation of identities with fingerprints, speech recognition to validate claims of origin, and analysis of smartphone data to validate itineraries. Additional efforts focused on creating structures and processes for innovation with emerging technologies, such as artificial intelligence and blockchain.[9] These structures and processes greatly facilitated the three stages of the FLORA project.

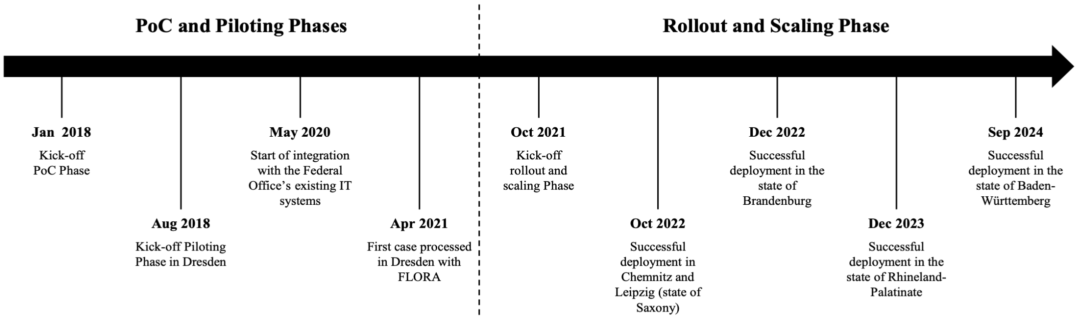
Stage 1. Proving that a Private Blockchain Could Avoid Building a Centralized System

The Federal Office for Migration and Refugees's interest in blockchain started in early 2018 due to its promises of decentralization, data integrity and transparency. It was particularly interested in the promise of decentralization because centralized IT architectures had proven challenging to implement across the multiple levels of government involved in the asylum procedure. Centralizing data storage and processing would usually require new laws and the redistribution of (technical) competencies. Germany's Central Register of Foreign Nationals (Ausländerzentralregister, or AZR),[10] with a user base of more than 6,000 agencies at the federal, state and local levels, was a painful case in point: any update to the AZR's data structure, such as a new data field, requires an update to the federal AZR law. Data integrity was a concern because the AZR had a history of not reliably ensuring that the right data was available in the right quality at the right time. Increasing transparency was essential to the Federal Office because two recent security incidents had highlighted how difficult it was to identify the status of an asylum application in real time. In the words of Marcus Richter, the Federal Office's then vice president:

[9] For more details on these initiatives, see *Digitisation Agenda 2022*, Federal Office for Migration and Refugees, available at https://www.bamf-digitalisierungsagenda.de/en/.

[10] For more details on the AZR, see *Data Collection: The Management of the Central Register of Foreigners*, Federal Office or Migration and Refugees, available at https://www.bamf.de/EN/Behoerde/Aufgaben/Datenerhebung/datenerhebung-node.html.

Figure 2: Timeline of the FLORA Project


PoC and Piloting Phases
Rollout and Scaling Phase
Jan 2018
Kick-off PoC Phase
Aug 2018
Kick-off Piloting Phase in Dresden
May 2020
Start of integration with the Federal Office's existing IT systems
Apr 2021
First case processed in Dresden with FLORA
Oct 2021
Kick-off rollout and scaling Phase
Oct 2022
Successful deployment in Chemnitz and Leipzig (state of Saxony)
Dec 2022
Successful deployment in the state of Brandenburg
Dec 2023
Successful deployment in the state of Rhineland-Palatinate
Sep 2024
Successful deployment in the state of Baden-Württemberg

> *"In recent years, we have had security incidents in Germany where we as the [Federal Office] have always asked ourselves what we can do to prevent such situations. If we have a logging layer, I can basically press a button and ... say exactly which [procedural step of the associated asylum case] took place when. And that has been our guiding idea, so to speak."*

Because blockchain promised to realize the vision of decentralization and support the requirements of multilevel, federal data processing,[11] the Federal Office conducted a proof of concept of FLORA during the first half of 2018, which eventually led to the rollout of the production system beginning in late 2021 (see Figure 2).

The proof of concept implemented a simplified asylum procedure with three agencies. It showed that an application based on a private blockchain had the potential to create substantial value for the Federal Office and its partner agencies because it provided the involved agencies with a "shared source of truth" of the status and progress of asylum applications. It also promised significant efficiency and privacy improvements over the use of Excel-based lists.[12] Marcus Richter elaborated on these expectations:

> *"In the future, we should no longer copy data into large nation-wide 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."*

Stage 2. Developing a Production Pilot with a State-Level Migration Agency

After successfully completing the proof of concept, the Federal Office decided to initiate a pilot project. The overarching goal of this project was to test if the expected value could be realized in day-to-day operations.[13] It would also establish if a private blockchain could meet the asylum procedure's strict privacy and security requirements. Due to the complexity of the

[11] Deeper insights into why private blockchains are suitable for Germany's asylum procedure can be found in Roth, T., Stohr, A., Amend, J., Fridgen, G. and Rieger, A. "Blockchain as a Driving Force for Federalism: A Theory of Cross-Organizational Task-Technology Fit," *International Journal of Information Management* (68), Article 102476, February 2023.

[12] The potential value is detailed in a proof-of-concept whitepaper: Fridgen, G., Guggenmos, F., Lockl, J., Rieger, A. and Urbach, N. *Supporting Communication and Cooperation in the Asylum Procedure with Blockchain Technology: A Proof of Concept by the Federal Office for Migration and Refugees*, Federal Office for Migration and Refugees, 2019.

[13] For details of the pilot project, see Amend, J., Arnold, L., Fabri, L., Feulner, S., Fridgen, G., Harzer, L., Karnebogen, P., Koehler, F., Ollig, P., Rieger, A., Schellinger, B., and Schmidbauer-Wolf, G.-M., *Federal Blockchain Infrastructure Asylum (FLORA)—Piloting and Evaluation of the FLORA Support System in the Context of the AnkER Facility Dresden*, Federal Office for Migration and Refugees, November 1, 2023.

asylum procedure's stages, the Federal Office limited the scope of the pilot project to a single state-level migration agency (State Directorate of Saxony—LDS) and the asylum procedure in Dresden, Saxony.

One challenge for the pilot project was to achieve compliance with the asylum procedure's privacy requirements. There were three components to this challenge. First, the requirements restrict the processing of procedural data unless there is an explicit legal basis for each act of data processing. Second, responsibilities for compliance need to be clearly identified and designated, especially when multiple agencies jointly control the processing of procedural data through a shared IT system, such as a private blockchain. Third, corrections have to be made when the procedural data is faulty, and the data needs to be erased after relevant legal bases for storing it expire. These requirements are difficult to reconcile with an append-only database, such as a blockchain. Nevertheless, the Federal Office managed to address all the challenges by combining a joint data processing agreement with a pseudonymization solution that erases the attribution of procedural information to an asylum applicant, rather than the information itself.[14]

Another challenge was ensuring compliance with federal IT security requirements. At that time, the federal government's reference framework for IT security did not cover decentralized IT systems such as private permissioned blockchains. This meant that the Federal Office needed to develop its own IT security framework for FLORA, including a comprehensive survey of potential risks and strategies to control or contain these risks.

Additional challenges arose from the limited resources and capabilities of the LDS. Originally, the Federal Office had intended to jointly develop and host the pilot system with the LDS. However, the LDS lacked both the financial and personnel resources for the project and was not interested in developing blockchain capabilities. Because the LDS would only support the Federal Office with functional requirements, the Federal Office had to take full responsibility for developing and hosting the FLORA pilot. In the words of a business analyst from the Federal Office:

> *"Sure, Saxony's central immigration agency, and any other agency, could technically host a blockchain node. But many, including Saxony's central immigration agency, do not really want this. The level of complexity in the governance, not necessarily in the technology, requires a different way of thinking and can be an impediment."*

Despite this rather one-sided development and hosting model, the FLORA pilot met all expectations and project endpoints by September 2021. These positive results encouraged the Federal Office to make FLORA a strategic priority and roll it out across Germany. In the words of Hans-Eckhardt Sommer, president of the Federal Office for Migration and Refugees:

> *"Projects like FLORA for faster information exchange with the [state-level migration agencies]—a project that is particularly close to my heart because the added value is immense, especially in times of high application numbers—contribute to our good reputation, especially with the [state-level migration agencies]."*

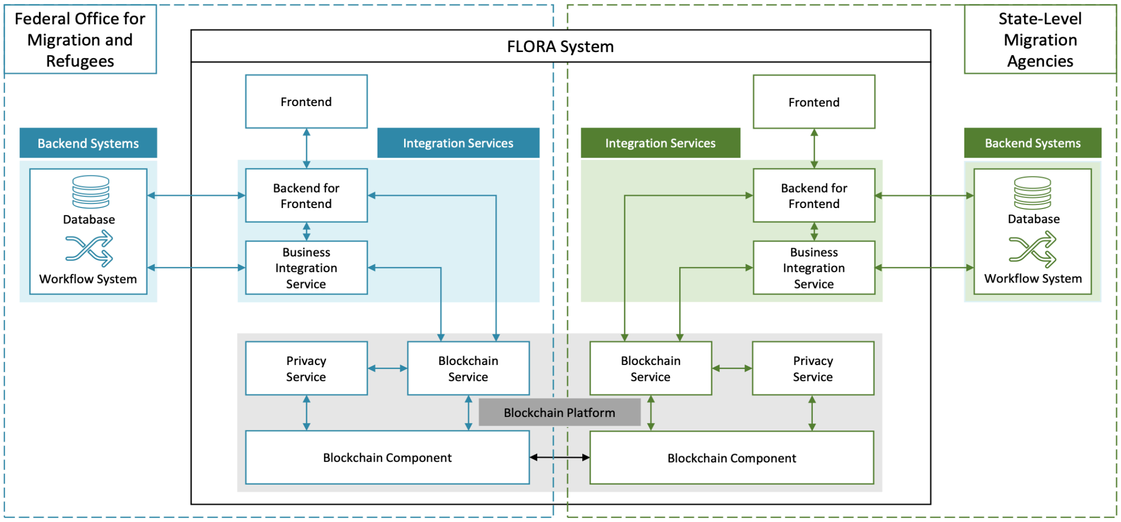
Stage 3. Rolling Out FLORA Across Germany's States

Most other state-level migration agencies shared the LDS's lack of interest in developing blockchain capabilities and hosting FLORA. To overcome this constraint, the Federal Office adopted a software-as-a-service (SaaS) model where it hosts FLORA instances for the state-level migration agencies and offers access to these instances through application programming interfaces (APIs) and the web-based FLORA frontend. A FLORA project consultant explained this model:

> *"We currently have a software-as-a-service model, which ultimately means that the Federal Office deploys a productive solution for [the state-level migration agencies]. It doesn't mean, however, that [the agencies] cannot influence the solution, make remarks*

[14] Further insights into these challenges and the Federal Office's solution strategy can be found in Rieger, A., Lockl, J., Urbach, N., Guggenmos, F. and Fridgen, G. "Building a Blockchain Application that Complies with the EU General Data Protection Regulation," *MIS Quarterly Executive* (18:4), December 2019, pp, 263-279.

Figure 3: FLORA's Two-Layer Architecture



> *or ask for personalization. It just means, from a purely technical perspective, that the Federal Office hosts the solution. Long-term, the aim is to develop [the model] into the direction of platform-as-a-service ... to push responsibilities back to the ... state agencies."*

However, the rollout sometimes proved more difficult than expected. Some state-agency employees required significant training and first-line user support to encourage them to adopt the new system. Others were wary when they did not see immediate benefits for their tasks, even if other users benefitted substantially. A Federal Office local unit head described how employees, who perceived substantial benefits, specifically requested a timely rollout:

> *"As a local unit, we communicate very often and very much with the [state-level migration agencies]. FLORA enables us to exchange a lot of data, which we urgently need for our processes in the local unit, on a daily basis with minimal effort. It is, therefore, a great wish—certainly for all local units—to use the technology as soon as possible."*

FLORA's Architecture

The FLORA system allows the state-level agencies to connect their backend databases and workflow management systems. FLORA's architecture has a different instance of the system for each agency, all of which are currently hosted by the Federal Office. Each FLORA instance has two layers: an integration services layer and a blockchain platform layer (see Figure 3).

The primary purpose of FLORA is to share asylum procedural information between the involved agencies. It provides a "shared source of truth" with secure, timely and reliable distribution and persistent tracking of process status messages.[15] For example, once the Federal Office has conducted an ID check, the backend system creates a FLORA API call to distribute the status message "ID check completed" to the other agencies involved in the specific asylum application. In cases where state-level backend systems are not yet fully connected to FLORA, status updates can be imported through .csv files or entered via the FLORA frontend.

[15] FLORA includes both overarching status messages and subprocess status messages. Overarching messages map the procedural logic defined by the Federal Asylum Act (and thus are the same in all of Germany's 16 states) and subprocess messages reflect local differences in the asylum procedure.

The integration services layer establishes links between the backend systems, the FLORA frontend and the blockchain platform layer. The business integration service (BIS) has two functions: it receives API calls from the backend systems, translates the calls into status messages and forwards the messages to the blockchain platform layer. Moreover, the BIS maps the identifiers used in the backend systems to unique procedure identifiers that are consistent across all involved agencies.[16] The backend for frontend (BFF) service handles user authentication, populates the FLORA frontend with information from the backend systems and the blockchain platform layer and writes status messages resulting from data entry in the FLORA frontend.

The blockchain platform layer has three components: The *blockchain service* acts as a service endpoint between the integration services and the *blockchain component* based on the Hyperledger Fabric framework, which is used for distributing and storing status messages.[17] Once a submitting agency writes a new status message into its blockchain component, it is shared with the blockchain component of the other agencies responsible for the specific asylum procedure.[18,19] Furthermore, the blockchain component uses smart contracts to validate authentication and compliance with a basic process model of the asylum procedure. However, it does not restrict deviations from the process model, as the asylum procedure is predicated on the accountability of human case handlers.

The *privacy service* addresses an important data privacy requirement—the right to erasure. Compliance with this requirement mandates that no personal data should be written to an "immutable" blockchain. However, all procedural data processed by the FLORA system is inherently personal. To address this challenge, FLORA employs a pseudonymization approach. The procedural data in the blockchain component is not linked to the FLORA ID but to a pseudonymous technical identifier. These technical identifiers are mapped to FLORA IDs in the privacy service. Erasing these mappings allows the procedural data to be anonymized in the blockchain component, which is a permissible way of erasure under the EU's General Data Protection Regulation (GDPR).

In cases where FLORA is not fully integrated with a state agency's backend systems, case handlers can use the FLORA frontend to get tabular overviews of various asylum procedures and their status. Based on this information, they can plan and complete the next steps in the procedure. Many of the tabular overviews also allow manual data entry and—by extension—the distribution of a new status message.

Governance of the FLORA System

In FLORA's SaaS model, state-level agencies can introduce requirements, propose changes and participate in the higher-level prioritization of new features. Lower-level prioritization and technical development decisions are the responsibility of the Federal Office. The same applies to technical decisions regarding the hosting of FLORA instances on the Federal Office's infrastructure. To avoid tensions arising from this strong centralization of decision rights, the Federal Office goes above and beyond to ensure that the concerns and suggestions of all state-level agencies are considered, and their specific requirements are met. It offers free workshops and training sessions, a FLORA support team, "office hours" with FLORA's project management team and runs joint feedback sessions with all participating state agencies.

In general, however, governance responsibilities are more distributed. Though the Federal Office is responsible for FLORA's privacy,

[16] To ensure that an asylum procedure can be initially identified by the FLORA system, several identification attributes are transmitted from the backend system of the submitting agency, together with the first status message (e.g., date of birth, personal number, application number). The FLORA ID is then generated by the BIS of the submitting agency and exchanged with the responsible partner agencies. These agencies then use their own BISs to map the FLORA ID with the IDs in their backend systems.

[17] The status messages are "tamper evident" (i.e., resistant to tampering) because all blockchain components also hold a copy of the hash values ("fingerprints") of all status messages written by the participating agencies.

[18] Status messages are distributed and stored in so-called "private data collections." These collections are special elements of the Hyperledger Fabric framework and allow status messages to be shared with a specific subset of participating agencies. All other agencies receive only a hash value of the status message.

[19] As responsibilities in the asylum procedure are clearly delineated and agencies do not have a legal basis for cross-validation, the blockchain component does not employ a consensus mechanism but a simple ordering mechanism.

Table 1: Summary of FLORA's Value for the Asylum Procedure

Area	Before FLORA	With FLORA
Sharing of procedural information	• Significant inefficiencies from Excel-based lists	• More efficient exchange of procedural information across agencies
Quality of procedural information	• Considerable effort to find and retrieve procedural information from different databases and files	• Significantly improved information accuracy and completeness because of a "single procedural source of truth"
Procedure timeline	• Slow because of long waiting and search times	• Time reduced by up to 50% because of substantial reductions of waiting and search times
Legal compliance	• Elevated risk of procedural errors, and difficulties complying with data protection requirements	• Reduced risk of procedural errors and better compliance with data protection requirements

security and availability, the GDPR and relevant asylum laws require that the responsibility for data processing is shared between the Federal Office's local units and the state-level agencies. FLORA's governance framework extends these responsibilities to first-level support and representing local needs in strategic feature-prioritization meetings.

To incentivize the adoption of FLORA, the Federal Office engages in outreach activities to emphasize the value of the system for different employee groups and funds customization and initial hosting. Once this "honeymoon" phase is over, costs for hosting are shared between the Federal Office and the state-level agencies. Moreover, the Federal Office provides technical support for agencies that want to use FLORA's APIs to directly connect their instance with relevant backend systems.

Value Provided by the FLORA System

After initial concerns, FLORA has been fully embraced by the Federal Office's local units and the state-level agencies. Users typically describe FLORA as a powerful and well-designed application that significantly improves day-to-day operations in four particular areas:

1. *Sharing of procedural information:* FLORA significantly reduces the inefficiencies inherent in Excel-based lists previously used. The system shares procedural information on the status and progress of individual asylum applications instantly, even during times of high influx and backlogs. Procedural information can be shared for individual asylum seekers or for entire batches. Where FLORA is integrated with the state agencies' backend systems, procedural information can flow directly between their backend systems.
2. *Quality of procedural information:* Before FLORA's introduction, case handlers often needed to consult different Excel-based lists and databases to obtain the relevant procedural information. This data was sometimes neither complete nor accurate. After the introduction of FLORA, case handlers now have a shared source of truth with complete, accurate and up-to-date procedural information. This information allows case handlers to better complete and plan subsequent steps in the procedure, such as booking transport capacities and interpreters for interviews.
3. *Procedure timeline:* Though FLORA does not automate any of the asylum procedure's steps, it significantly reduces waiting and search times. In some cases, the time scale for the initial stages (up to the personal interview) can be reduced by up to 50%. These efficiency gains have a positive impact, especially on state-level agencies that are often stretched thin in terms of personnel. With FLORA, they can remain productive even in times of high influx and backlogs.

4. *Legal compliance:* Before FLORA's implementation, the risk of procedural errors was often high, and compliance with data privacy requirements was difficult. With FLORA, errors arising from missing or false information have become rare, and meeting data privacy requirements is easy. For instance, FLORA works with automated timers to delete procedural information, removing the need to clear outdated Excel-based lists.

Table 1 summarizes the value added by FLORA in each of these areas.

Recommendations for Building Intergovernmental IT Systems

Government services can be difficult to digitalize when they require cooperation and coordination between agencies across multiple levels of government that, for legal reasons, have to maintain distinct IT systems. Though the resulting barriers to joint innovation are daunting, they can be overcome, as Germany's FLORA project demonstrates. Based on insights from the FLORA project, we provide three recommendations for successfully building intergovernmental IT systems.

1. Determine the Suitability of Decentralized Over Centralized Solutions

Introducing new IT systems that support collaboration within and across levels of government is challenging as heterogeneous legacy systems often complicate data exchange and coordination. The natural response may often be to build a "cost-effective" centralized system that reduces this complexity. However, there may be substantial hidden costs in creating a new centralized IT system to coordinate multiple levels of government agencies. For example, before building such a system, any laws that prohibit centralized data storage and processing would need to be changed. Standardization costs can also be substantial when local procedures and data models must be compared and aligned, and new data repositories created and maintained.

These hidden costs may often be higher than the cost of developing, hosting, and maintaining a decentralized solution. Germany's asylum procedure is a case in point. The Central Register of Foreign Nationals (the AZR) serves as a constant reminder of the hidden costs of using centralized IT architectures, including substantial costs for updating and aligning laws. By adopting the concept of decentralized data sharing, the FLORA system avoids these costs because it removes the need for new legislation. Moreover, FLORA does not require substantial standardization costs because there is not a need to align local variants and data models of the asylum procedure. It leaves these variants and models untouched but offers opportunities to selectively share best practices from the Federal Office's local units.

2. Deploy Modular Solutions to Break Up Multilayered Legacy Architectures

A second fundamental challenge for building intergovernmental IT systems is the complex, multilayered nature of many legacy IT systems. New levels of legal requirements are typically implemented with new layers of technology, while complexity reduction remains a secondary concern. Too often, this results in legacy IT systems that are more difficult to adapt and extend than the legal frameworks they support. Though updates and new IT systems cannot eliminate complexity resulting from meeting legal requirements, they can make an essential contribution to easing maintenance and updating by emphasizing loose coupling and modularity over messy, multilayered architectures and efficient data exchange over replicated storage. Over time, adhering to these principles can successively break down complex IT architectures and encapsulate those parts of legacy systems that are difficult to maintain and replace.

FLORA represents an important step in this direction. It emphasizes complementarity and does not replicate legacy system data. Instead, it uses this data to generate procedural updates that can be used to improve the exchange and use of the already available data. Moreover, FLORA is designed to ensure that its individual components can be easily maintained, updated and replaced with different technologies and frameworks. For instance, it uses the Hyperledger Fabric framework for procedural data sharing and storage because it addresses the demands of multilevel government data processing. However, this blockchain platform layer component can be easily replaced if another similarly convenient, albeit less complex, option becomes available.

Data sources	Description
Semi-structured interviews	98 interviews, recorded, transcribed and coded using grounded theory methods
Documents	1,000+ pages of project documentation: • Conceptual and legal documents (200+ pages) • Meeting minutes, technical documentation and user support documents (600+ pages) • Whitepapers and evaluation reports (200+ pages)
Observations	Observations from regular sprint reviews, project workshops, management meetings and events

3. Start with a Software-as-a-Service Model and then Gradually Move to a Flexible Integration Model

Funding and organizing the development of shared IT systems for multilevel government services can be difficult. The legal separation of competencies will usually require that technical and financial responsibilities match the legal framework. In the short run, this matching exercise can paralyze digital transformation efforts. Yet for innovation efforts to progress, it may sometimes be advisable for a single agency to temporarily take the lead and initially assume a large share of the technical and financial responsibilities (we call this the "one-for-all" approach). Once the new IT system is mature enough, other agencies can begin to allocate the required resources and redistribute responsibilities.

The FLORA project is an interesting example of how the "one-for-all" approach can be implemented. The Federal Office for Migration and Refugees not only assumed the technical and financial responsibility for developing the FLORA system but also initially adopted a free SaaS model that allowed state-level agencies to immediately use the system. In due course, each agency can then decide on the desired level of integration with its legacy systems and initiate the required budgeting, contracting and staffing processes. This gradual transition from a SaaS model to flexible integration drastically lowers the usual adoption barriers.

Concluding Comments

FLORA brings together Germany's Federal Office for Migration and Refugees and the state-level migration agencies. It creates substantial value by improving the exchange and quality of asylum procedure information between these agencies, by reducing search and wait times, and by minimizing the risks of errors and data privacy violations. FLORA's success hinges on its ability to bridge between legally separated legacy systems. It is designed in a modular way that leverages the decentralization and controlled information-sharing features of a private, permissioned blockchain but also allows for its replacement should a better technological option become available.

Appendix: Research Method

We chose an inductive research design to develop an in-depth understanding of how governments can bring their services into the digital age. Specifically, we conducted a longitudinal single-case study[20] of Germany's FLORA project for coordinating the asylum procedure.

We chose the FLORA project because it provides valuable insights and rich data for studying how government agencies can successfully collaborate on building intergovernmental IT systems. We directly observed the FLORA project and collected data over six years, from the project's inception in early 2018 to its rollout in several states in Germany. Three of the co-authors provided academic advisory services to the FLORA project. The first two accompanied the projects

[20] For more information on case study research, see Yin, R. *Case Study Research: Design and Methods*, SAGE Publications, 2017.

for about two years and were primarily tasked with conducting an in-depth evaluation of the FLORA pilot system and its later rollout. The third accompanied the project from January 2018 and was primarily tasked with advising on the conceptualization of the system.

Our close involvement in the project enabled us to gather rich data from multiple sources. Our primary source was 98 interviews conducted at different points in the project between 2018 and 2024. Because we had closely accompanied and evaluated the project since its inception in January 2018, we were also able to draw on project documentation (1,000+ pages) and direct observations to triangulate our findings. The table provides an overview of the collected data sources.

About the Authors

Julia Amend

Julia Amend (julia.amend@fim-rc.de) is a business developer at a German insurance company, where she creates digital, data-driven business models and works on data governance topics to facilitate more needs-oriented customer interactions using AI-based approaches. In her research, she explores how organizations can successfully manage digital innovation, with a special focus on blockchain technology. Her research has appeared in *International Journal of Information Management* and *e-Business Management*. She holds a Ph.D. in information systems from the FIM Research Center, University of Bayreuth, and a master's degree in business administration.

Simon Feulner

Simon Feulner (simon.feulner@fim-rc.de) is a research associate at the Branch Business & Information Systems Engineering of the Fraunhofer FIT. His research focuses on the impact of decentralized technologies, such as blockchain and self-sovereign identity, the concept of digital trust and design science, and has been published in *Electronic Markets* and *Information and Management*. He is currently a Ph.D. student in information systems at the FIM Research Center, University of Bayreuth; he holds master's degrees in business administration and information systems.

Alexander Rieger

Alexander Rieger (arieger@walton.uark.edu) is an assistant professor of information systems in the Sam M. Walton College of Business at the University of Arkansas. His research focuses on innovation with emerging technologies in highly structured contexts and has been published in *Journal of the Association for Information Systems*, *Information & Organization*, *MIS Quarterly Executive*, *Nature Human Behavior*, *Nature Machine Intelligence* and *International Journal of Information Management*. He has years of experience working in industry and consulting for the European Commission and public and private sector organizations in Germany and Luxembourg. He holds a Ph.D. and a master's degree in information systems.

Tamara Roth

Tamara Roth (troth@walton.uark.edu) is an assistant professor of information systems in the Sam M. Walton College of Business at the University of Arkansas. Her research explores how emerging technologies can be leveraged to promote social good and achieve positive organizational change. Tamara's work has appeared in *MIT Sloan Management Review*, *Journal of the Association for Information Systems*, *Journal of Information Technology*, *Government Information Quarterly*, *International Journal of Information Management*, *Nature Human Behavior and Nature Machine Intelligence*. She has an interdisciplinary education with Ph.D. degrees in educational psychology and information systems and master's degrees in biology and education.

Gilbert Fridgen

Gilbert Fridgen (gilbert.fridgen@uni.lu) is a full professor and the PayPal-FNR PEARL Chair in Digital Financial Services at the Interdisciplinary Centre for Security, Reliability, and Trust (SnT), University of Luxembourg, and coordinator of the National Centre of Excellence in Research on Financial Technologies. In his research, he analyses the transformative effects of digital technologies on individual organizations as well on the relationship between organizations. He focuses especially on emerging technologies like distributed ledgers, digital identities, machine learning and the internet of things.

Tobias Guggenberger

Tobias Guggenberger (tobias.guggenberger@fit.fraunhofer.de) is a postdoctoral researcher at the University of Bayreuth, Germany, and the Branch Business & Information Systems Engineering of Fraunhofer FIT. In his research, he explores the design and management of information systems, leveraging emerging technologies like artificial intelligence and blockchain. He currently focuses on exploring the impact of decentralization and distributed decision-making on the collaborative and value-creation practices of firms. His work has appeared in *IEEE Transactions on Engineering Management*, *Electronic Markets and Computers & Industrial Engineering*. He holds a Ph.D. in information systems and a master's degree in business administration.