

Federal Blockchain Infrastructure Asylum (FLORA)

Piloting and evaluation of the FLORA support system in the context of the Anker facility Dresden

Information Technology

Federal Blockchain Infrastructure Asylum (FLORA)

Piloting and evaluation of the FLORA support system in the context of the AnkER facility Dresden

Whitepaper, authored by the Branch Business & Information Systems Engineering of the Fraunhofer FIT and the Interdisciplinary Centre for Security, Reliability, and Trust of the University of Luxembourg

Federal Office for Migration and Refugees 2022

Summary

The Federal Office for Migration and Refugees (BAMF) and Saxony's State Directorate (LDS) have collaborated at the AnKER facility in Dresden to lay the groundwork for a Federal Blockchain Infrastructure Asylum (FLORA). The collaboration has resulted in a new blockchain-based support system for cross-authority cooperation in the German asylum procedure. The FLORA support system not only helps to improve procedural steps. It also reduces the risk of procedural errors. Moreover, it strengthens data protection and offers safeguards against manipulation. Overall, FLORA is a flagship project for the use of blockchain technology in public administration and may be considered a digital enabler of federalism.

After an initial feasibility study, the BAMF and LDS first developed an innovative architecture that complies with the requirements of the General Data Protection Regulation (Fridgen et al. 2019). This architecture was then refined and integrated into the systems of the two participating authorities. After a training and testing period, the FLORA support system was piloted successfully at the AnKER facility in Dresden over the summer of 2021.

A key element of this pilot was an extensive evaluation of the value added by the FLORA support system. To determine this value, the BAMF evaluated the supported procedural steps in a qualitative and quantitative manner before

as well as after the introduction of the FLORA support system.

Comparing the ex-ante and ex-post data reveals significant improvements that can be attributed to the introduction of the FLORA support system. The most notable is an increased availability and transparency of procedure-relevant information, which reduces both manual workload and communication overhead. Furthermore, the examined procedural steps became significantly less error-prone, and the corresponding activities far more efficient. Finally, the FLORA support system not only ensures more consistent compliance with data protection requirements. It also provides an essential impetus for innovative and constructive cooperation throughout the asylum procedure.

Based on these positive results, the BAMF is planning further development of the FLORA support system. It has already begun a broad roll-out to further sites in Saxony and Brandenburg. This roll-out is not limited to a particular type of facility (AnKER facilities, arrival centers, field offices, etc.). Instead, it focuses on opportunities to optimize the collaboration at all sites. In addition, the BAMF is involved in the European Blockchain Partnership and the development of the European Blockchain Services Infrastructure (EBSI) to advance the idea of FLORA supranationally.

Contents

1. Motivation.....	2
2. First experiences with blockchain in the asylum procedure.....	2
3. Focal points of the FLORA project.....	4
3.1. Further development of FLORA's architecture	4
3.1.1. Blockchain-Platform.....	4
3.1.2. Integration Services	7
3.1.3. Backend Systems Layer	8
3.2. Implemented procedural logic and functionality	9
3.3. Data protection in the application	10
4. Evaluation of the FLORA support system.....	10
4.1. Evaluation aims	10
4.2. Evaluation procedure.....	12
4.3. Evaluation results.....	12
4.4. Conclusion	15
5. Outlook	16
Bibliography.....	17

1. Motivation

IT projects are important foundations for many modernization efforts in public administration because they can achieve efficiency gains in the respective administrative processes and improve communication with citizens (Federal Government 2021). This digitalization potential can also be unlocked for the asylum procedure, yet challenges remain in getting the various involved authorities to cooperate in a smooth and efficient manner – particularly when it comes to the exchange of procedural information and sensitive data.

Existing IT systems, such as the AZR – a central database for the storage of master data and documents – do not fully unlock the digitalization potential as they were neither designed nor intended to support the coordination of the asylum procedure. Moreover, Germany's federal structure subjects the asylum procedure to numerous state-specific legal requirements, procedural variants, and a heterogeneous IT infrastructure. It has also made it impossible to centralize control within a single authority, such as the Federal Office for Migration and Refugees (BAMF). Procedure-relevant information is thus often exchanged between the involved authorities in the form of Excel spreadsheets sent by email. This type of information exchange, however, is cumbersome, time-consuming, and prone to errors.

Decentralized IT systems designed for coordination, control, and documentation – should the latter be required – hold considerable promise in dealing with these challenges. Meanwhile, cross-authority automation and monitoring of processes are neither desirable nor feasible due to the federal distribution of responsibilities and competencies.

With these considerations in mind, the BAMF has done extensive research into the use of blockchain technology. The BAMF was especially interested in how the technology could add value by improving cross-organizational communication and cooperation

in the asylum procedure. An initial feasibility study demonstrated that blockchain technology could indeed be instrumental in this regard (Fridgen et al. 2018a; Fridgen et al. 2018b) (in short: FLORA Whitepaper I). Based on this feasibility study, the BAMF designed a GDPR-compliant architecture for a blockchain-based pilot system (Fridgen et al. 2019) (in short: FLORA Whitepaper II).

After further development loops and an initial training and testing phase, the FLORA support system was trialed in a successful pilot that started in April 2021, and the system is now in productive use. The pilot, which involved employees of the AnKER facility in Dresden, was accompanied by a comprehensive evaluation to analyze whether the FLORA support system meets the expectations placed on it.

This whitepaper presents the refined blockchain architecture of the FLORA support system, the implemented procedural logic and functionality, as well as the technical realization of data privacy requirements. Furthermore, this whitepaper presents the conducted evaluation along with the quantitative and qualitative evaluation results. A brief outlook then indicates the future activities planned for the FLORA project.

Also, this document presents the third in a series of FLORA whitepapers. Best practices developed during the FLORA project and the lessons learned in its course are available both in the form of a book chapter and as a fourth 'best practices' whitepaper (Amend et al. 2021) (Amend et al. 2022).

2. First experiences with blockchain in the asylum procedure

Germany's asylum procedure requires close cooperation and a secure exchange of information between various authorities at the municipal, state, and federal levels. While the BAMF – as a federal authority – is responsible

for processing and ruling on asylum applications, the states and municipalities are responsible for the initial registration, accommodation, care, and social support, as well as the eventual integration or repatriation of the applicant. In addition, multiple security agencies carry out background checks.

This federal organizing structure poses a challenge to the management of the asylum procedure. In some cases, it leads to considerable local variations in procedural logics, which complicates cooperation. What is more, it results in a heterogeneous IT landscape, which is why information on the status of individual asylum procedures is still frequently exchanged in the form of (excel) lists and e-mails.

To manage the resulting complexity, a system is required that can be accessed jointly by the involved authorities (at the municipal, state, and federal levels) and that facilitates cross-authority process coordination. Meanwhile, using conventional IT systems with a centralized architecture would pose the following challenges:

- (1) There would be no legal basis for the introduction of a centralized IT architecture (even at a purely technical level, considerable legal adjustments would be required), and such an IT architecture is undesirable for all parties involved in the procedure.
- (2) A centralized IT architecture that needs to support various local sub-processes would be unnecessarily complex, making long-term operation difficult.

Faced with these challenges, the BAMF is working on decentralized technical alternatives that do not require a single authority to coordinate the procedure. Based on a preliminary consideration of various technical options, the BAMF decided to conduct a proof-of-concept study to evaluate blockchain technology for its capacity to coordinate the asylum procedure. In the course of this study, the BAMF created a blockchain prototype for a simplified asylum procedure with three simulated authorities. This prototype used a blockchain component to log the completion of critical procedural steps and share this information with the other responsible authorities. This simplified asylum procedure was then mapped with the use of programming logic – so-called smart contracts – that enabled the automated triggering of subsequent process steps. The outcome of this proof-of-concept study was that a blockchain solution would have several advantages for the asylum procedure in Germany – both functional and technical:

- (1) A blockchain solution can enable a “shared truth” among the responsible authorities about the status and progress of individual asylum procedures. Through blockchain, information could be passed on quickly and securely.
- (2) A blockchain solution can facilitate the coordination of the various authorities involved in the asylum procedure.
- (3) A blockchain solution can support the federal organizing structure and strengthen the data sovereignty of the participating authorities.

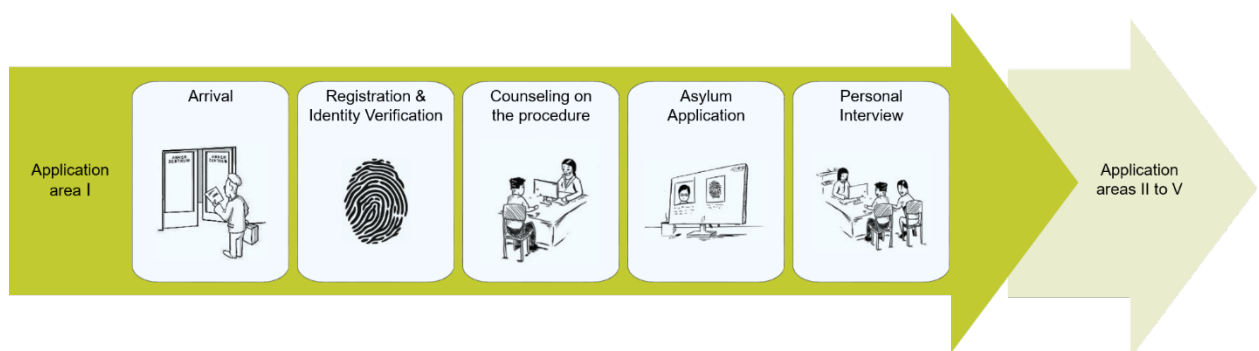


Figure 1: Simplified schematic representation of application area I

Based on the positive evaluation of the prototype, the BAMF decided to expand its blockchain efforts and test the technology in a pilot project, starting in the summer of 2018.

The overall objective of this pilot project was to test whether a Federal Blockchain Infrastructure Asylum (FLORA) could ensure the efficient, transparent, and secure completion of the German asylum procedure. Furthermore, the pilot was meant to answer questions about acceptance and technical optimization.

Due to the complexity of the German asylum procedure, the scope of the pilot project was limited to two authorities (the BAMF itself and Saxony's State Directorate (LDS)) and their collaboration in the context of the AnKER facility in Dresden. The key feature of the AnKER concept is the pooling of all functions and responsibilities in one place: from arrival and initial registration to the asylum application and the ruling on local distribution and integration or repatriation of asylum seekers¹. Importantly, the AnKER facility is only one exemplary form of collaboration that FLORA can support.

Moreover, the scope was limited to three 'application areas' where communication had previously been highly time-consuming and full of 'media disruptions', suggesting room for improvement. In the further course of the project, two additional application areas were identified, application area IV ("Return counseling") and application area V ("Dublin"). All five of these application areas were conceptualized but only application area I was implemented to reduce technical complexity for the pilot project. For the purpose of completeness, Figure 1 provides an overview of all application areas, albeit somewhat simplified:

(1) Application area I: "Registration, file creation, and hearing"

(2) Application area II: "Accommodation and allocation to counties and municipalities"

(3) Application area III: "Decision and execution"

(4) Application area IV: "Return counseling"

(5) Application area V: „Dublin“

While the proof-of-concept study evaluated the potential benefits of using blockchain technology (see FLORA Whitepaper I), the pilot project focused on the successful implementation of data privacy requirements (see FLORA Whitepaper II). Moreover, the pilot project sought to test the FLORA support system in day-to-day operation, which was accompanied by a comprehensive evaluation.

3. Focal points of the FLORA project

3.1. Further development of FLORA's architecture

The refined architecture of the FLORA support system consists of three levels: (1) **Blockchain Platform**, (2) **Integration Services**, and (3) **Backend Systems** (see Figure 2). The overarching purpose of the blockchain-based system is to make status updates on the asylum procedure available across various authorities.

3.1.1. Blockchain-Platform

The **Blockchain Platform** comprises three elements: the *Blockchain Service*, the *Privacy Service*, and the *Blockchain Component*. It is designed uniformly across all authorities. A detailed overview of the Blockchain Platform can be found in Figure 3.

Blockchain Service

The *Blockchain Service* is connected to the *Blockchain Component* and enables reading status messages as well as writing them to the

¹ For more information on the asylum procedure at the

AnKER facility in Dresden, see [FLORA Whitepaper II](#).

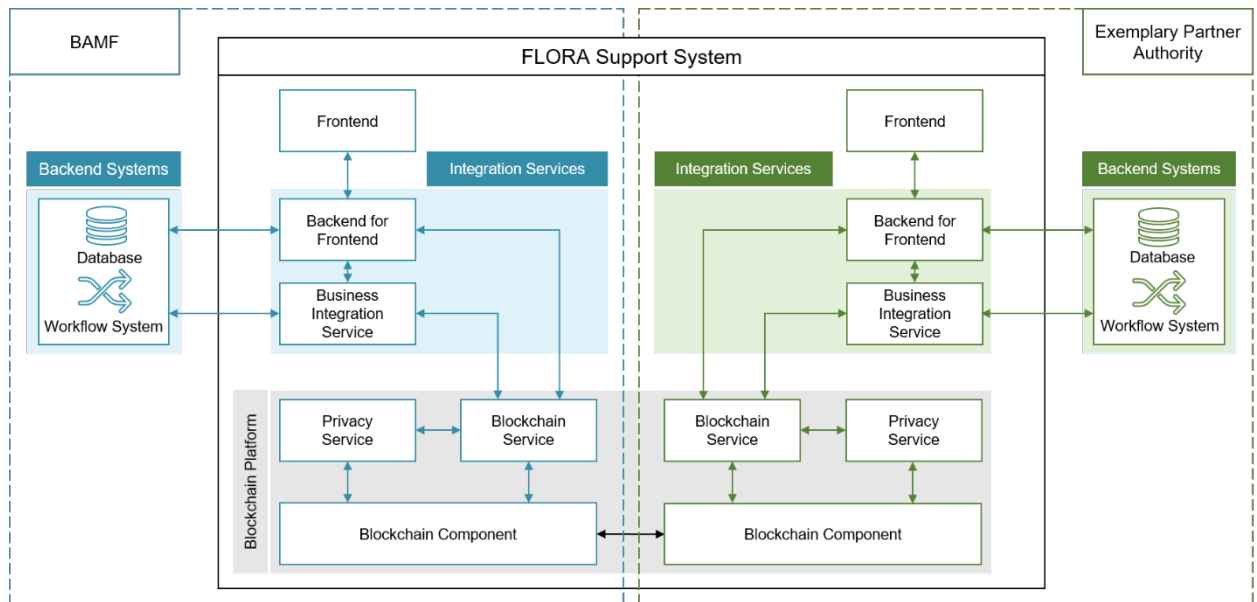


Figure 2: Refined architecture of the FLORA support system

Blockchain Component. The *Blockchain Service* interacts with the *Privacy Service* to establish a connection between Blockchain-IDs and FLORA-IDs. The Blockchain-ID is a ‘technical’ key for status messages. In contrast, the FLORA-ID acts rather as a cross-authority ID for individual asylum procedures. For a more detailed explanation of the Blockchain-ID and the FLORA-ID (see explanation field).

Privacy Service

All status messages must be attributable to the respective asylum procedure, and this has to be doable for all authorities authorized to view these status messages. This attribution is done via the so-called *Privacy Service*. All authorities connected to the FLORA support system have their own instance of this *Privacy Service*, yet each of these is uniform. Specifically, the *Privacy Service* establishes a mapping between a FLORA-ID and the associated Blockchain-IDs. Each FLORA-ID can have one or more Blockchain-IDs assigned to it. A new Blockchain-ID is generated for each application area. This is done to satisfy data privacy requirements concerning visibility and erasure limits. A transfer of responsibility also triggers the generation of a new Blockchain-ID. This ensures that all status messages generated after such a transfer can then only be viewed by the now responsible authorities.

Blockchain-ID and FLORA-ID

The Blockchain-ID is a technical key for status messages, comparable to the primary key of a database. In contrast, the FLORA-ID facilitates unified attribution to an individual procedure across all authorities and is thus more of a cross-authority application ID.

As soon as a new procedure is opened in FLORA, the Business Integration Service of the ‘creating’ authority generates a FLORA-ID, whereupon the authority’s *Privacy Service* creates a Blockchain-ID. Meanwhile, the *Business Integration Service* links the backend system IDs (e.g., the Federal Office uses a combination of the MARiS file number and person number) with the FLORA-ID and then the FLORA-ID with the Blockchain-ID.

As a general rule, a new Blockchain-ID is generated for each new application area. This rules out the possibility that, once the data has been anonymized on the blockchain, the details of entire procedures could be retrieved across several application areas based on their Blockchain-ID. Furthermore, this allows to set different erasure limits for each application area, depending on the purpose that data processing in this area serves.

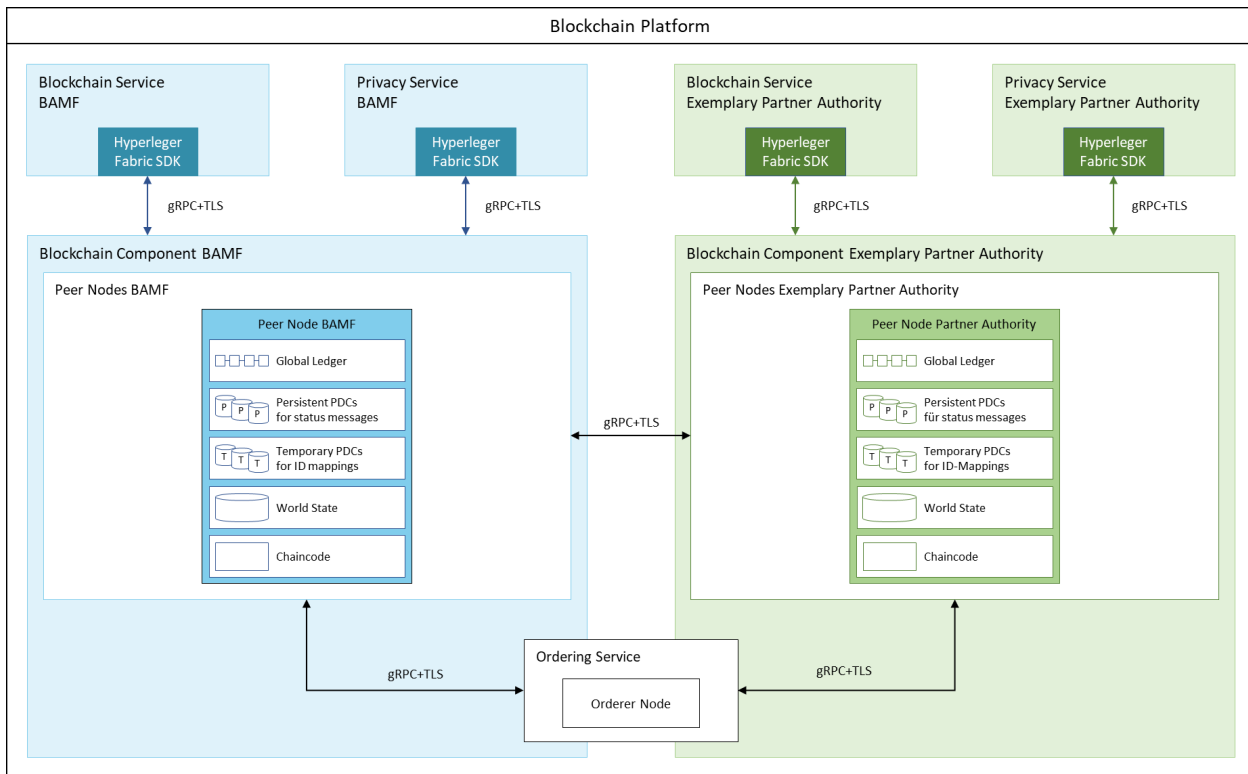


Figure 3: FLORA Blockchain Platform

Blockchain Component

To ensure secure, timely, and reliable distribution as well as joint and persistent tracking of status messages across all authorities, the FLORA support system employs *Blockchain Components* for distribution and storage purposes, with transactions recorded through a decentralized database structure. Since data stored on a blockchain cannot be manipulated, modified data must be distributed through a new transaction.

Status messages written into a *Blockchain Component* by a participating authority are distributed in encrypted form to all other responsible authorities. The data can then be viewed by these authorities according to their local and subject matter competencies. The status messages are tamper-resistant as all *Blockchain Components* hold a copy of the hash values ("fingerprints") of all status messages written by the participating authorities. Each hash value is deterministic and builds on the previous one, creating a chain. A subsequent change to a status message would be evident to all involved authorities because the manipulated entry would change the hash value. The

subsequent hash values would then fail to refer to the manipulated status message and invalidate the chain. "Plain text" data, on the other hand, is only shared between the *Blockchain Components* of the responsible authorities. This sharing is done in a timely manner and ensures that the authorities currently responsible for an individual asylum procedure have the same information.

Furthermore, Blockchain Components are able – with the help from a smart contract – to prevent deviations from a default procedural logic or to document them fully. Specifically, this smart contract maps selected sections of the cross-authority procedure at the AnKER facility in Dresden in the form of a status machine. Based on this status machine, a notice concerning any potential deviation from the default procedural logic can be generated and sent to users.

The *Blockchain Components* comprise two essential elements of the Hyperledger Fabric framework: peer nodes (one peer node per organization) and an ordering service with a single orderer node. The peer nodes are the key storage elements that track status message

distribution and check the procedural logic. The orderer node compiles the hash values of status messages in blocks and distributes them to all peer nodes.

Each peer node has the following sub-components.

Global Ledger:

The *Global Ledger* contains a blockchain with the hash values of all status messages. These status messages are written to the relevant *persistent Private Data Collections (PDCs)* by the authorities participating in the network. Each authority has a copy of the *Global Ledger*. These copies are always kept synchronized to ensure that participating authorities have an identical copy of the *Global Ledger*.

Private Data Collection

So-called "Private Data Collections" are used to realize data separation and thus also data privacy. They are special elements of the Hyperledger Fabric Framework and allow to submit transactions to the blockchain network while specifying which authority can store and process the data in plain text per their legal competencies. All other network participants receive only a hash value of the transaction via the blockchain protocol.

Persistent PDCs for status messages:

Persistent PDCs are private ledgers. These are only accessible to subsets of the participating authorities, depending on their local and subject matter competencies. Status messages are shared as 'plain text' data via these private ledgers. To ensure that all participating authorities of a *persistent PDC* have an identical copy of the *PDC* at all times, the copies are always kept synchronized, analogous to the *Global Ledger*.

Temporary PDCs for ID mappings:

For each *persistent PDC*, there is a *temporary PDC* with the same group of participants. These *temporary PDCs* are used to exchange

mappings between Blockchain-IDs and FLORA-IDs. For the initial mapping, *temporary PDCs* are also used to transmit the date of birth and the AZR number. This is done to enable the responsible partner authorities to identify the correct procedure. After a certain period, the removal of the oldest block automatically deletes the mappings in the *temporary PDCs*. To again ensure that all authorities participating in a temporary PDC have an identical copy of this PDC at all times, the copies are always kept synchronized the same way as the *Global Ledger* and *Persistent PDCs*.

World State:

The *World State* is a CouchDB document database that replicates a current snapshot of the *Global Ledger* and the PDCs to facilitate efficient querying of all the data contained in the *Global Ledger* and PDCs. The World State is stored on the peer node of each authority and has sub-areas for the peer node's *Global Ledger* and PDCs. Should the *World State* be manipulated or no longer accessible, it is reconstructed based on the *Global Ledger* and the PDCs.

Smart Contract (Chaincode):

Each peer node has a copy of the smart contract which contains, among other things, the status machine and a platform-level roles and rights concept, as defined by the participating authorities. A smart contract is called chain code in Hyperledger Fabric.

3.1.2. Integration Services

Meanwhile, the data input to the Blockchain Platform and the preparation of the data for the employees' *Frontend* are managed by the **Integration Services**. These include the *Backend For Frontend (BFF)* and the *Business Integration Service (BIS)*.

Backend For Frontend

The *Backend For Frontend (BFF)* forms the link between the *Frontend* and the **Backend Systems Layer** as well as the link between the *Frontend* and the **Blockchain Platform**. The *BFF* authenticates users of the *Frontend*.

Furthermore, the *BFF* is responsible for writing status messages transmitted from the backend systems (MIW Datagrid (MARiS) in the BAMF's case) or from the *Frontend*. It also enriches status messages that are transmitted from the *Blockchain Component*. This data enrichment consists of backend system data that is required for a given read or write use case (e.g., MARiS master data in the BAMF's case).

Business Integration Service

The *Business Integration Service* establishes a connection to the backend systems of the participating authorities. The backend system IDs used in the BAMF's backend systems or in those of other authorities, such as personal identification numbers or application numbers, are mapped to the FLORA-IDs in the *BIS* and stored in so-called mapping tables. This mapping is necessary because various authorities use varying identifiers in their backend systems, and these identifiers may change over time. However, collaboration with FLORA requires a common and stable identifier.

The two final elements worth discussing here are the **Backend Systems Layer**, which includes, for instance, the workflow management system MARiS in the case of the BAMF or the

application ASSIST in the case of the LDS, and the *Frontend*.

3.1.3. Backend Systems Layer

Rather than replace existing IT systems, the FLORA support system connects them in what is effectively a "technical bracket". In doing so, it harmonizes the fragmented IT landscape. BAMF employees, for example, can continue to use the MARiS workflow and document management system, and LDS employees can continue to use the ASSIST application. No time-consuming data migration or system changes are required. Meanwhile, access to the databases and workflow management systems remains limited to employees of the respective authority. As for the information that has to be accessed by multiple parties to enable cross-authority collaboration, this is exchanged via the *Blockchain Platform*. Once it has been enriched with data from the individual backend systems, it can be displayed via the *Frontend*.

Frontend

The *Frontend* offers various options to interact with the *Blockchain Component*. The retrieval and storage of FLORA data can be partially or fully integrated into existing systems. It can also be done via a separate dashboard, depending on the requirements. For the pilot phase of the

The screenshot displays the 'Terminierung beim BAMF (Gesamtübersicht)' page. It features a table with columns for 'Personenzahl', 'MARIS-Az.', 'ZAB-Nr.', 'Sprache', 'Staatsangehörigkeit', 'Bearbeitung', 'ID-Check: Datum', 'ID-Check: Zeit', 'AVB: Datum', 'AVB: Zeit', 'AA: Datum', and 'AA'. The table contains 24 entries. The interface includes a 'Spaltenkonfiguration' dropdown, a 'Zurück zur Startseite' link, and a 'Datensätze drucken' button.

Personenzahl	MARIS-Az.	ZAB-Nr.	Sprache	Staatsangehörigkeit	Bearbeitung	ID-Check: Datum	ID-Check: Zeit	AVB: Datum	AVB: Zeit	AA: Datum	AA
-	7028941	941941	Arabisch	475, Syrien, Arabische Republik	Bearbeitbar					Erliegt	
-	7026926	926926	Spanisch	367, Venezuela	Bearbeitbar	Erliegt		02.08.2022	02:00	04.08.2022	
-	7034076	925925	Russisch	160, Russische Föderation	Bearbeitbar	Erliegt		Angeboten		Erliegt	
-	7026145-1	815815	Russisch	160, Russische Föderation	Bearbeitbar	Erliegt					
2	6479799	799799	KURDISCH-BADNANI	438, Irak	Bearbeitbar	Erliegt		04.08.2022	02:00	Erliegt	
2	6479799	799799	KURDISCH-BADNANI	438, Irak	Bearbeitbar	Erliegt		04.08.2022	02:00	Erliegt	
-	6162691	691691	Arabisch	475, Syrien, Arabische Republik	Bearbeitbar					02.08.2022	
-	6194657	617657	Arabisch	475, Syrien, Arabische Republik	Bearbeitbar					Erliegt	
-	7033538	538538	Georgisch	430, Georgien	Bearbeitbar	Erliegt		04.08.2022	02:00		
-	7025067	535535	Arabisch	475, Syrien, Arabische Republik	Bearbeitbar			03.08.2022			

Figure 4: Frontend of the FLORA support system from the BAMF's point of view

FLORA project, a separate dashboard was chosen to avoid overheads for extensive integration. In the future, separate dashboards can also be a good option for other authorities to test the FLORA support system or put it into operation without delay.

The structure of the *Frontend* is based on various use cases, which can be differentiated into read and write use cases: with regard to read use cases, the *Frontend* provides tabular overviews of various asylum procedures at a particular stage of the process. In the BAMF *Frontend* (see Figure 4), these overviews can include data from both the BAMF *Blockchain Component* and MARiS. For write use cases, the *Frontend* offers corresponding views to generate new status messages and save them in the *Blockchain Component*.

3.2. Implemented procedural logic and functionality

The FLORA support system creates a "shared knowledge base" through secure, timely, and reliable distribution and persistent tracking of status messages. These status messages are designed to facilitate the sharing of granular process information relevant for the coordination of asylum procedures at a given site. Moreover, they enable the involved authorities to identify additional information requirements early on and exchange that information through the available communication channels.

Technically speaking, the FLORA support system has a process library with a hierarchical structure of application areas, status categories, and status messages. The application areas are structured into functional status categories and each category comprises one or several status messages. For example, application area I includes the status category "asylum application", which in turn includes various status messages, such as "asylum application submitted" and "asylum application in process". This structure makes it possible to implement a default procedural logic that supports process integrity.

Moreover, a distinction is made between overarching status messages and sub-process status messages. While overarching status messages map the procedural logic defined by the Federal Asylum Act, which is why they are designed to be uniform throughout Germany, sub-process status messages are designed for individual sites, which is why they can reflect regional differences in the asylum procedure. Each status category includes at least one overarching status message.

The three-part structure of application areas, status categories, and status messages is also relevant to meet the requirements of the General Data Protection Regulation (GDPR), especially the need for storage limitation and data minimization. Due to these requirements, the *Blockchain Component* also only stores selected status messages.

To support cross-authority coordination, individual overviews regarding stored status messages can be retrieved. The BAMF, for instance, may wish to look at an overview of open procedures that require the creation of an application file. The overviews allow the LDS and the BAMF to remain updated on the status of procedures that are currently being processed at the other authority. Based on this information, they can then plan and execute their next procedural steps. What is more, they can retrieve the history of a specific asylum procedure.

Ideally, status messages are written to the blockchain "automatically" from the backend systems. In individual cases where no appropriate interface existed in the backend systems (and could not be provided at short notice), the FLORA pilot facilitated manual entry via the *Frontend*. As for the implementation of the respective read and write rights, this required concepts for roles and rights at the blockchain and the frontend level. On the blockchain level, roles and rights are managed based on an organization logic. On the frontend level, a separate concept was created that assigns roles and rights based on the respective tasks and responsibilities of the employees.

In each application area, there are various defined dependencies and rules concerning status messages, status transitions, and the corresponding effects (e.g., new status, parallel status messages, no changes). These rules and dependencies are reflected in the status machine and can be changed via simple configuration files. This status machine, meanwhile, is part of the smart contract.

3.3. Data protection in the application

A key requirement for the FLORA support system that goes beyond matters of functionality is data protection. In particular, the support system must meet the requirements of the General Data Protection Regulation (GDPR) because personal data is being processed.

Essential requirements of the GDPR include that clear responsibilities are designated, the lawfulness of personal data processing is established, and all rights to rectification and erasure are upheld. In general, these requirements require both technical and organizational measures (Guggenmos et al. 2020; Rieger et al. 2019).

The most important technical measure in the FLORA support system is a two-layer pseudonymization by means of the *Business Integration Service* and the *Privacy Service*. Further efforts were dedicated to the development of a rectification and erasure concept (FLORA Whitepaper II). This concept ensures the rights to rectification and erasure of personal data (Articles 16 and 17 GDPR) through specific rectification and erasure transactions on the blockchain. In addition to these technical measures, great emphasis was placed on effective governance to ensure effective distribution of responsibilities for complying with the requirements of the GDPR.

As part of the pilot project, the BAMF was able to establish several best practices for the implementation of a GDPR-compliant blockchain architecture. Moreover, the initiative to engage in exchanges with relevant

stakeholders early on in the development of the architecture proved to be a key success factor in resolving sensitive issues, such as data privacy but also IT security. To name but one example, this involved the early consultation of the Federal Commissioner for Data Protection and Freedom of Information (BfDI).

4. Evaluation of the FLORA support system

4.1. Evaluation aims

The purpose of the concurrent evaluation was to examine the extent to which the FLORA support system is able to improve particular aspects of the asylum procedure at the AnKER facility in Dresden. For this evaluation, various qualitative and quantitative data points were collected and analyzed. In a first step, the ‘to-date’ processes were analyzed to better understand the status quo (ex-ante analysis). They were then analyzed a second time after the introduction of the support system (ex-post analysis). In a third step, the evaluation was completed by comparing observations and values before and after introducing the FLORA support system.

For the FLORA project, various (high-level) goals were defined that guided the evaluation process. Specifically, eight evaluation dimensions were defined, each with an applicable evaluation methodology (qualitative and/or quantitative data collection and analysis):

(1) Flexibility (qualitative):

This dimension assesses the ability to adapt parts of the procedure while maintaining its effectiveness and efficiency. Adaptations may be required in response to changes in general conditions, new laws or regulations, or changes to the group of involved partners. Another flexibility aspect is adaptability in terms of how individual cases are handled (although the decision on how to complete a particular asylum procedure remains with the individual

employee). ‘Project-related’ flexibility is an important third aspect that ensures the ability to remain flexible when dealing with changing conditions during the development of the FLORA support system. Finally, the dimension covers the ability to map a broad range of procedural variants, which requires a great deal of ‘technical’ flexibility.

(2) Innovation capability (qualitative):

The dimension ‘innovation capability’ focuses on the capability to manage innovations or to initiate them. Innovations can be characterized as planned and controlled changes in a system through the implementation of new ideas and capabilities, such as the use of (digital) technologies. Specifically, the FLORA support system introduced blockchain as a new innovative capability to improve the asylum procedure. The degree of innovation capability can be determined, among other things, by an organizations’ innovation potential and climate, such as the degree to which an organization works both in an agile and interdisciplinary way.

(3) Integrity (quantitative & qualitative):

The dimension ‘integrity’ focuses on the integrity of each procedural step and evaluates the extent to which it can be performed in a predefined manner. A high level of integrity can be characterized by the absence of inadmissible procedural deviations (when the procedure deviates from an ‘ideal’ path, such as interchanged procedural steps) or procedural errors (when procedural steps are missing or incompletely executed). Furthermore, integrity requires any such deviations or errors to be documented in detail and in a comprehensible manner. Compliance with the lawfulness of each procedural step is also essential. Integrity is thus an important indicator whether confidence is warranted that all necessary steps in the asylum procedure are carried out correctly and in the right order.

(4) Communication & cooperation (quantitative & qualitative):

The dimension ‘communication & cooperation’ is essential for authorities such as the BAMF

that have organizational structures characterized by departmental boundaries and geographical separation. Communication, which can take various forms, is particularly important for the successful and efficient cooperation in the AnKER facility in Dresden.

(5) User satisfaction (qualitative):

The dimension ‘user satisfaction’ assesses the degree to which users are satisfied with the prior systems, the newly introduced FLORA support system, and the associated changes. The relevant users for this dimension are the employees tasked with the procedural steps under examination as they stand to experience immediate benefits, such as potential simplification and relief in their work, and as they are directly affected by the introduction of the new system. User satisfaction is also reflected in employee acceptance.

(6) Legal certainty (quantitative & qualitative):

The dimension ‘legal certainty’ results from the requirement that legal norms are clear, consistent, predictable, and that their application as well as the associated legal obligations and authorizations are guaranteed. In particular, legal certainty requires that data protection is always guaranteed during the procedure. Moreover, information quality is essential – especially for procedural steps with a broad range of data sources and information users. Information has to be available to the person requiring it at the time it is required, and it has to be of the required quality. The FLORA support system aims to make this happen across authority boundaries.

(7) Speed (quantitative & qualitative):

The dimension ‘speed’ assesses whether the use of the FLORA support system results in any efficiency gains. Such gains can only be achieved when updated knowledge about the status of an individual asylum procedure and other necessary information related to it are immediately available across authority boundaries. A higher degree of information availability could reduce the waiting times between procedural steps performed by

different authorities. It could also help accelerate or coordinate the overall procedure. The dimension also assesses 'to-date' circumstances for employees and identifies potential procedural bottlenecks that could be improved.

(8) Transparency (qualitative):

The dimension 'transparency' evaluates the degree to which the asylum procedure, especially the history of an individual asylum procedure, is traceable in a compact, complete, and almost real-time manner. The project's guiding vision is to realize these improvements through the FLORA support system. Each participating authority is to receive the same knowledge on the status of individual asylum procedures - in full appreciation of data privacy concerns and the respective competencies of the authorities.

4.2. Evaluation procedure

To ensure a rigorous and relevant evaluation of how the FLORA support system, the evaluation was limited to application area I ("Registration, File Creation, and Hearing") at the AnKER facility in Dresden. The application area was analyzed in a quantitative and/or qualitatively manner with regard to the eight dimensions discussed above.

For the quantitative analysis, anonymized data points were collected for several dimensions. This collection was done manually on evaluation forms by BAMF employees who worked directly or indirectly with the FLORA support system as part of their activities in application area I ("Registration, file creation, and hearing"). The data points were then processed in an anonymized manner by employees of the Branch Business & Information Systems Engineering' of the Fraunhofer FIT. Crucially, these employees did not have a direct supervisor relationship with the BAMF employees. As a result, both anonymity and neutrality could be guaranteed.

Meanwhile, the qualitative data points were collected by means of semi-structured interviews (approx. 30 minutes) conducted with

an interview guide. The interviewees were BAMF employees involved in application area I at the AnKER facility in Dresden. To ensure broad coverage, the interviews were held not only with employees who were directly involved in process steps aided by the FLORA support system, but also with employees who were merely indirectly involved.

The evaluation was conducted in two phases. The first phase covered the status quo in each of the eight dimensions prior to the introduction of the blockchain-based system (ex-ante). The second phase focused on the procedural details after the introduction (ex-post). In both evaluation phases, the data points were collected over several weeks to create as large a sample as possible and in doing so ensure the reliability as well as the validity of the evaluation's results. It is also worth noting that the ex-post data collection was not done until after those working with the FLORA support system had been given a transition and acclimatization period of an adequate duration to prevent potential falsification of results.

The ex-ante evaluation was conducted in the spring of 2020, the ex-post evaluation in the summer of 2021. In each phase, more than 120 asylum procedures were traced, which resulted in a sufficiently large sample to perform a reliable evaluation. Furthermore, in each phase of the evaluation, 10 interviews were conducted with employees involved in the various process steps in application area I.

4.3. Evaluation results

In each of the eight dimensions, the introduction of the FLORA support system led to (significant) improvements. An overview of these improvements is presented in Table 1, which shows that they were either notable or even very notable.

The following pages offer a more detailed discussion of the evaluation results for each of the eight dimensions.

Dimension	
Flexibility	Strong
Innovation capability	Very strong
Integrity	Very strong
Communication & cooperation	Very strong
User satisfaction	Strong
Legal certainty	Strong
Speed	Very strong
Transparency	Very strong

Table 1: Overall result of the evaluation of the FLORA support system

Flexibility

The FLORA support system allows for procedural deviations to ensure that employees can continue to make decisions based on legal and factual considerations. At the technical level, the FLORA support system provides a great deal of standardization as well as the necessary degree of freedom. Regarding project-related flexibility, a promising structure was created that facilitates a high degree of flexibility in working on the various parts of the project.

>> Process flexibility: If there are sound reasons to deviate from the implemented procedural logic, employees can choose not to adhere to it. Furthermore, the procedural logic can be flexibly adapted, for example, due to changed circumstances.

>> Technical flexibility: The FLORA support system provides as much standardization as possible. This is achieved, for instance, with the use of the Hyperledger Fabric framework. At the same time, a high degree of flexibility is maintained to adequately consider functional requirements.

>> Project-related flexibility: The project's agile approach made it possible to flexibly react to changes and implement new requirements quickly in sprints and user stories.

Innovation capability

In general, the FLORA support system is perceived as (very) innovative by the interviewed employees (4.5 points; see Figure 5). Particularly noteworthy were the uniqueness of the project and the early adoption of new technology. Furthermore, the interviewees emphasized that the FLORA project is more than just an IT project. Indeed, there was consensus that blockchain can help to strengthen trust, establish a new kind of collaboration, and enable users to jointly implement a grand vision. Overall, the FLORA project was found to be a bold and worthwhile endeavor.

Integrity

The use of the FLORA support system also leads to a higher degree of 'integrity'. It automatically provides warnings about procedural deviations and documents them. Furthermore, the FLORA support system significantly improves the quality of procedure-related information.

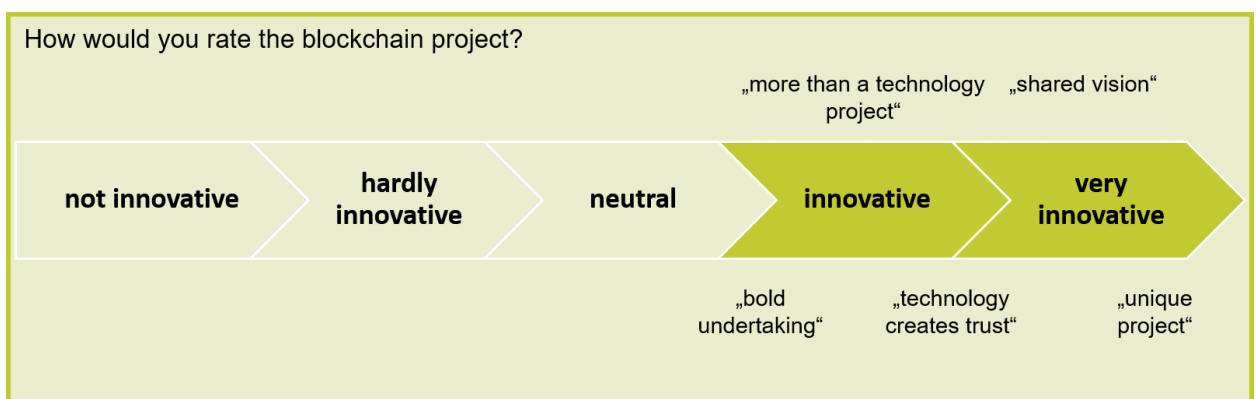


Figure 5: Assessment of how innovative the FLORA support system appears from the employees' point of view

>> **Warnings:** Employees now receive more IT support – this support is especially notable for planning activities.

>> **Process deviations:** The FLORA support system facilitates automatic documentation of procedural deviations and errors, which enables employees to detect and correct potentially undesirable deviations from the default procedural logic at an earlier point and with greater ease.

>> **Information quality:** The quality of procedure-relevant information has improved considerably as efforts to minimize susceptibility to errors have proven successful. Further improvements have been made to the quantity of data as the status and history of an individual asylum procedure are now easier to track. In some cases, there is even access to information that goes beyond individual procedural steps.

Communication and cooperation

Communication and cooperation have been notably simplified and improved by the FLORA support system as it reduces media disruptions and makes information more extensively and directly available to all parties involved in the procedure.

>> **Media disruptions:** The FLORA support system has not only made it easier to keep track of the procedure. It has also reduced the likelihood of errors as the frontend now provides a single point for data entry and processing that can be used across organizational boundaries in line with the users' local and subject matter competencies.

>> **Information availability:** As soon as a responsible person has entered a piece of information, it is almost instantly available for further processing by other responsible persons and authorities.

>> **Cross-authority database:** The FLORA support system brings together relevant information, creating a common database that can be used by multiple authorities as a trustworthy repository.

User satisfaction

By and large, user satisfaction with the FLORA support system is high. In addition, various potentials for improvement could be identified.

>> **Usability:** The FLORA support system is clearly and intuitively designed. However, some isolated cases still required avoidable clicks during the pilot phase.

>> **Work facilitation:** The FLORA support system supports employees and makes it significantly easier for them to accomplish their daily tasks, for example, by reducing the complexity of various procedural steps.

>> **Availability and stability:** The FLORA support system contained some minor software errors, especially at the start of the pilot phase. However, most of these have since been corrected.

Legal certainty

The FLORA support system simplifies compliance with data protection requirements and makes procedure-related information more transparent. In doing so, it helps establish a consistent level of information among authorities and increases the legal certainty of the asylum procedure.

>> **Data privacy requirements:** Thanks to the FLORA support system and in its predefined rules for deleting information, it is now easier to comply with data protection requirements.

>> **Transparency:** The FLORA support system makes it easier to obtain information about the status and history of an individual asylum procedure, and it enables multiple authorities to share this information with one another.

Speed

The FLORA support system contributes to a significantly accelerated procedure. In particular, the overall duration of application area I could be reduced by more than half across all existing constellations. However, the collected data is not conclusive on the extent to which this was accomplished by the FLORA

support system alone, nor is it entirely clear how otherwise optimized procedural steps contributed to this improvement. Nonetheless, the substantial reduction in the duration of the procedural steps in application area I suggests that the FLORA support system has a significant impact. Different aspects can explain the acceleration of the procedure:

- (1) The clearer and earlier distribution of information makes it possible to plan ahead, which in turn makes it possible to process cases sooner. For example, superfluous appointments can then be canceled earlier, whereupon these vacated time slots can be filled with other persons.
- (2) Waiting times and layovers between procedural steps are eliminated.
- (3) The automation of procedural steps helps employees to process individual procedures more quickly (e.g., due to the elimination of "copy & paste" activities in Excel lists or the manual filling of these Excel lists).
- (4) Time spent searching for the status of a particular file or the current step of the procedure can be reduced significantly. This reduction is achieved by the lower complexity and greater clarity of the FLORA support system, compared to the various Excel lists and emails used previously.

Transparency

Finally, the FLORA support system has made a significant contribution to improved transparency in the asylum procedure. It establishes a better and consistent level of information not only within but also across authority boundaries, which facilitates the planning of procedural steps.

>> Current status and history: Viewing the status and history of an individual asylum procedure is now easy and intuitive for the participating authorities, their access being limited only by their roles and rights.

>> Same level of information: Establishing a shared level of information across authority boundaries had always been complicated. The

FLORA support system now offers a shared, trustworthy database that contains all relevant information.

>> Planning activities: Due to the transparency facilitated by the FLORA support system, and due to its early provision of information, it is now far easier for authorities to plan procedural steps in advance.

4.4. Conclusion

The evaluation of the FLORA support system confirms that blockchain technology adds the expected value in application area I ("Registration, file creation, and hearing"). Positive changes are evident across all evaluation dimensions and can be substantiated with qualitative and quantitative data.

The introduction of the FLORA support system has a particularly positive effect on data and process quality, as it simplifies procedural steps and offers more IT support. Furthermore, it significantly reduces manual data entry and the procedure's duration. The acceleration results, among other things, from the improved availability and transparency of procedure-relevant information. Moreover, the FLORA support system's predefined rules for the erasure of information ensure a more stringent observance of data protection requirements.

Yet, certain aspects of the FLORA support system will require future adjustments. For one, the connection with the backend systems will need to be improved to support scalability. Furthermore, the pilot operation revealed new technical requirements and the need for different functionalities, all of which will have to be examined and prioritized for possible future implementation.

In summary, the FLORA support system meets the expectations placed on it to an exceptionally high degree and delivers significant added value. As the evaluation has shown, the introduction of a blockchain-based support system is more than just a technology project. Instead, blockchain technology offers an opportunity to reshape federal collaboration in a fundamental way. In effect, the piloting the FLORA support

system demonstrates that a blockchain-based system can be valuable for the coordination of activities in federal contexts and support cooperation across authority boundaries.

5. Outlook

Based on the successful piloting of the FLORA support system, further expansion stages are now under way, which are briefly presented below.

Expansion of the federal blockchain infrastructure asylum at the national level

At the first stage of expansion, the FLORA support system will be rolled out to further sites and authorities. This roll-out will initially include the other Saxon sites in Chemnitz and Leipzig as well as sites in the State of Brandenburg. Furthermore, in-depth discussions have been initiated with the Ministry for Children, Family, Refugees, and Integration of the State of North Rhine-Westphalia (MKFFI) regarding participation in the project and the subsequent use of the FLORA support system. Initial coordination talks have also taken place with the Karlsruhe

Regional Council (RPK) of Baden-Württemberg. Meanwhile, other German states have expressed interest in participating at later stages of expansion.

Beyond this expansion to different sites and German states, the scope of the FLORA support system will be extended. Specifically, this involves adding application areas II to IV, all of which have already been designed, albeit not yet implemented.

Support for the Dublin procedure

As part of its work on application area V, the BAMF has assumed the convenor role for a working group that will explore and test the possible use of the European Blockchain Services Infrastructure for the Dublin procedure. This working group will mirror select elements of the FLORA support system.

The working group has already begun initial conceptualization work, and the BAMF is currently in discussions with the French government regarding the implementation of a prototype for the coordination of the Dublin procedure.

Bibliography

Amend, Julia; Arnold, Laurin; Feulner, Simon; Fridgen, Gilbert; Köhler, Franziska; Ollig, Philipp et al. (2022): Chancen und Herausforderungen des Einsatzes von Blockchain in der öffentlichen Verwaltung. Erkenntnisse aus dem FLORA-Projekt des Bundesamtes für Migration und Flüchtlinge. With assistance of Institutsteil Wirtschaftsinformatik des Fraunhofer FIT, Interdisciplinary Centre for Security, Reliability and Trust der Universität Luxemburg, Bundesamt für Migration und Flüchtlinge. Edited by Bundesamt für Migration und Flüchtlinge (Nürnberg). in Kürze erscheinend.

Amend, Julia; van Dun, Christopher; Fridgen, Gilbert; Köhler, Franziska; Rieger, Alexander; Stohr, Alexander; Wenninger, Annette (2021): Using Blockchain to Coordinate Federal Processes: The Case of Germany's Federal Office for Migration and Refugees. In Nils Urbach, Maximilian Röglinger, Karlheinz Kautz, Rose Alinda Alias, Carol Saunders, Martin Wiener (Eds.): Digitalization Cases Vol. 2. Cham: Springer International Publishing (Management for Professionals), pp. 85–100.

Federal Government (2021): Koalitionsvertrag 2021. Available online at <https://www.bundesregierung.de/breg-de/service/gesetzesvorhaben/koalitionsvertrag-2021-1990800>, checked on 11/16/2022.

Fridgen, Gilbert; Guggenmos, Florian; Lockl, Jannik; Rieger, Alexander; Urbach, Nils (2018a): Unterstützung der Kommunikation und Zusammenarbeit im Asylprozess mit Hilfe von Blockchain. With assistance of Project Group Business & Information Systems Engineering of the Fraunhofer FIT. Edited by Bundesamt für Migration und Flüchtlinge. Available online at <https://www.fim->

[rc.de/Paperbibliothek/Veroeffentlicht/842/wi-842.pdf](https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/842/wi-842.pdf), checked on 11/16/2022.

Fridgen, Gilbert; Guggenmos, Florian; Lockl, Jannik; Rieger, Alexander; Urbach, Nils; Wenninger, Annette (2019): Entwicklung einer datenschutzkonformen Blockchain-Lösung im deutschen Asylprozess. Pilotierung im Kontext der AnkER-Einrichtung Dresden. With assistance of Project Group Business & Information Systems Engineering of the Fraunhofer FIT. Edited by Bundesamt für Migration und Flüchtlinge. Available online at <https://www.bamf.de/SharedDocs/Anlagen/DE/Digitalisierung/blockchain-whitepaper.htmlblob=publicationFile>, checked on 11/16/2022.

Fridgen, Gilbert; Radszuwill, Sven; Urbach, Nils; Utz, Lena (2018b): Cross-Organizational Workflow Management Using Blockchain Technology: Towards Applicability, Auditability, and Automation. Available online at <https://orbi.lu.uni.lu/handle/10993/44527>.

Guggenmos, Florian; Lockl, Jannik; Rieger, Alexander; Wenninger, Annette; Fridgen, Gilbert (2020): How to Develop a GDPR-Compliant Blockchain Solution for Cross-Organizational Workflow Management: Evidence from the German Asylum Procedure. In Tung Bui (Ed.): Proceedings of the 53rd Hawaii International Conference on System Sciences: Hawaii International Conference on System Sciences.

Rieger, Alexander; Guggenmos, Florian; Lockl, Jannik; Fridgen, Gilbert; Urbach, Nils (2019): Building a Blockchain Application that Complies with the EU General Data Protection Regulation. In *MIS Quarterly Executive* 18 (4), pp. 263–279. DOI: 10.17705/2msqe.00020.

Disclaimer

This whitepaper was prepared by the Branch Business & Information Systems Engineering of the Fraunhofer Institute for Applied Information Technology FIT, the Interdisciplinary Centre for Security, Reliability, and Trust of the University of Luxembourg, and the staff of the Federal Office for Migration and Refugees to the best of their knowledge and with due care.

Fraunhofer FIT, the Interdisciplinary Centre for Security, Reliability, and Trust of the University of Luxembourg, the German Federal Office for Migration and Refugees, their legal representatives and/or agents do not warrant that the contents of this whitepaper are secure, fully usable for any particular purpose, or otherwise free of errors. The use of this whitepaper is solely at the user's own risk.

In no event shall Fraunhofer FIT, the Interdisciplinary Centre for Security, Reliability, and Trust of the University of Luxembourg, and the German Federal Office for Migration and Refugees, their legal representatives and/or agents be liable for any damages, whether direct or indirect, resulting from the use of this whitepaper.

The comments reflect solely the view of BAMF employees and do not necessarily correspond to the view of the Federal Office for Migration and Refugees.

Imprint

Publisher:

Federal Office for Migration and Refugees
90461 Nuremberg

Authors:

Branch Business & Information Systems Engineering of the Fraunhofer FIT, Interdisciplinary Centre for Security, Reliability, and Trust of the University of Luxembourg, and staff of the Federal Office for Migration and Refugees

Status:

02/2023

Printed by:

Federal Office for Migration and Refugees
90461 Nuremberg

Design:

Branch Business & Information Systems Engineering of the Fraunhofer FIT and Interdisciplinary Centre for Security, Reliability, and Trust of the University of Luxembourg

Image credits:

Cover image: © Shutterstock; Figure 4: © BAMF (Dashboard); remaining figures: © Fraunhofer FIT

Recommended citation:

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. 2022. Federal Blockchain Infrastructure Asylum (FLORA) - Piloting and evaluation of the FLORA support system in the context of the AnkER facility Dresden. Branch Business & Information Systems Engineering of the Fraunhofer FIT, Interdisciplinary Centre for Security, Reliability, and Trust of the University of Luxembourg, and Federal Office for Migration and Refugees, ed. Federal Office for Migration and Refugees (Nuremberg)

How to order:


BAMF Publication Office
www.bamf.de/DE/Themen/EMN/Publikationen/publikationen-node.html

This publication can be downloaded as a barrier-free PDF document.

This publication is issued by the Federal Office for Migration and Refugees as part of its public relations work. The publication is distributed free of charge and is not intended for sale.

Visit us at

 www.facebook.com/bamf.socialmedia

 @BAMF_Dialog

www.bamf.de/blockchain

