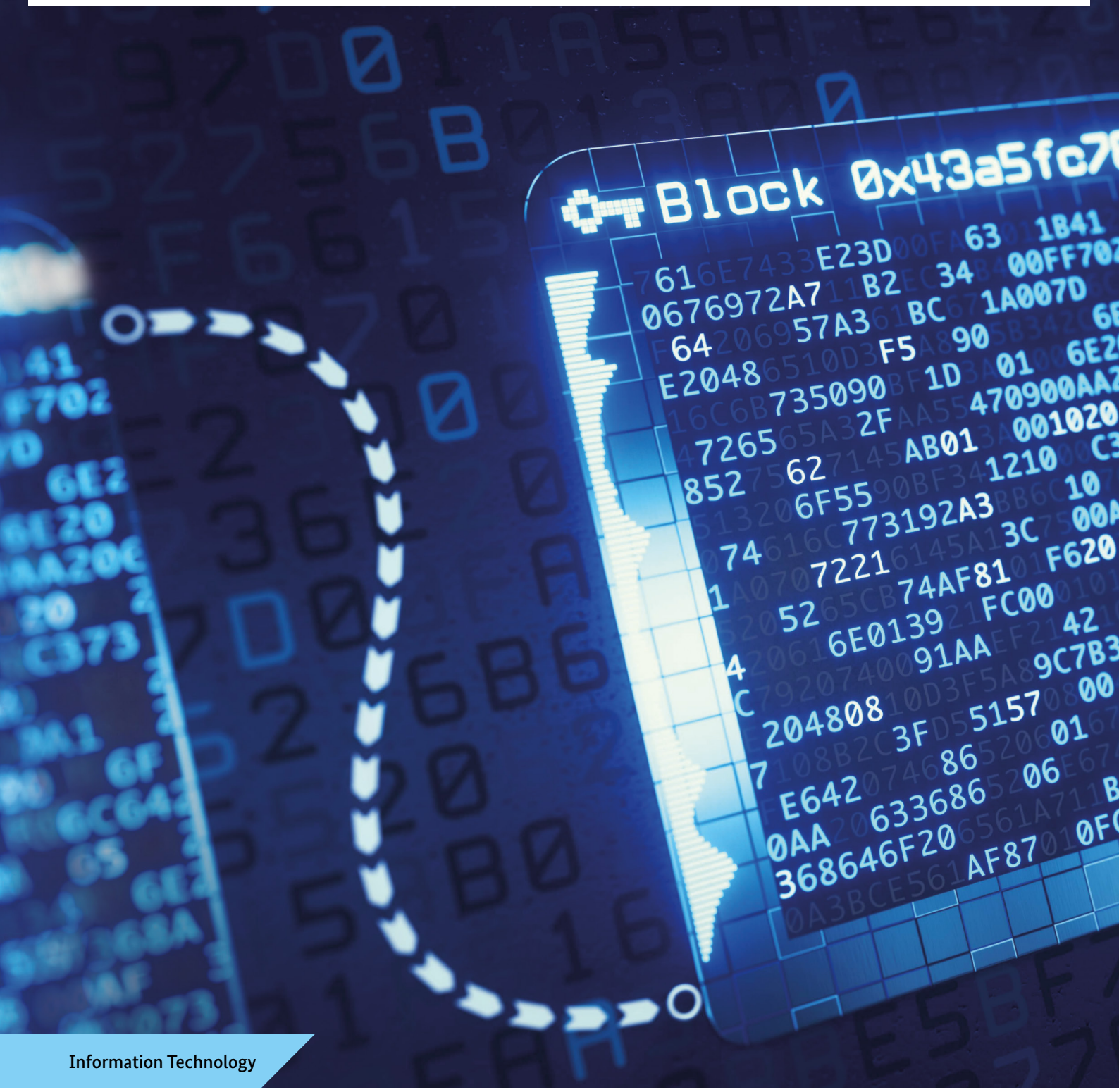
Federal Office for Migration and Refugees

Fraunhofer FIT

Development of a GDPR-compliant blockchain solution for the german asylum procedure

A pilot project in the context of the AnkER-facility in Dresden



Information Technology

ASYL Blockchain

Development of a GDPR–compliant blockchain solution for the german asylum procedure

A pilot project in the context of the AnkER-facility in Dresden

Whitepaper of the project group business & information systems engineering of the Fraunhofer Institute for applied information technology FIT

Federal Office for Migration and Refugees 2019

Abstract

Digital transformation involves reconsidering existing processes, establishing new ways of working, and promoting innovative ways of thinking. Moreover, digital transformation can play an important role in improving the fragmented system landscape of Germany's administration which increasingly poses challenges to municipal, state, and federal authorities. In this context, one of the digital focus technologies is the distributed ledger technology and its most prominent representative: blockchain technology.

The use of distributed ledger technology represents a deliberate departure from consolidation approaches, the objective being to mirror the federal structures and principles of Germany's administration in its digital infrastructure. Blockchain is particularly helpful when it comes to process optimization within federal structures where in-depth communication and close cooperation are required in spite of strong organisational heterogeneity.

The German asylum procedure is a case in point. A large number of different federal and state authorities are involved in the asylum procedure. Particularly at the state level, there are various sub-processes at work, which makes central control by a single workflow management system virtually impossible. What the German asylum procedure requires instead is a coordinated approach and a distributed IT solution that distributes process updates to all participating authorities in a secure and speedy fashion that will allow said authorities to initiate coordination measures independently and whenever necessary.

Based on a proof-of-concept (PoC), the Federal Office for Migration and Refugees has already confirmed that blockchain technology can provide a very promising basis for such an IT solution. Special potential has been recognised in its ability to establish a common and persistent information status across various authorities with great speed and security. Meanwhile, overcoming trust barriers between authorities is of little importance in the asylum procedure.

Now the technology shall also demonstrate its suitability in a pilot project. To do so, a blockchain solution for the Dresden AnkER facility is currently being developed in collaboration with Saxony's State Directorate.

The Federal Office expects the use of this blockchain solution to facilitate an exchange of information in the sub-processes 'registration, creation of an application file and personal interview', 'referral', and 'ruling and next steps'. This exchange of information is to be timely and fully digital, significantly minimising the duration of procedures and the expenditure of resources. Meanwhile, security aspects could be considered more efficiently, document procurement could be brought forward to an early point in the process, and repatriation could be organised sooner. As for cases in which asylum is granted, the process of integration could be set in motion faster by way of

earlier assignment to the competent municipality.

Already, the pilot project is nearing successful completion of the conception phase. In this phase, special attention has been given to the implementation of a system architecture that, in the current assessment of the Federal Office, complies with the relevant data protection regulations. At the same time, a concept for rectification and erasure was developed in order to meet the requirements and rights of data subjects codified in the General Data Protection Regulation.

In addition, a governance concept was designed in line with data protection laws in order to regulate the distribution of decision-making powers and responsibilities at the technical and organisational level. The core issues regarding scalability were addressed in a scalability concept.

As for the bigger picture, with a view to this being a lighthouse project, the Federal Office saw an opportunity in the conceptualisation phase to work on a multitude of general design principles that apply to the development of blockchain solutions in other areas of public administration.

Should this success continue through the development and evaluation phases, various expansion scenarios are conceivable. In the first step, for instance, further sub-processes could be mapped out at the AnkER facility in Dresden. Alternatively, further authorities in the asylum procedure could be included, a measure which in time may facilitate a pan-European solution. If applied in the asylum context, blockchain would thus serve as the ‘digital enabler’ of European federalism and may very well constitute a further step towards a united, fully integrated Europe.

Table of content

Table of figures

1. Motivation

Digital transformation involves reconsidering existing processes, establishing new ways of working, and promoting innovative ways of thinking (Gimpel and Röglinger 2015). The German asylum procedure stands to benefit in the same way.

Said procedure involves a large number of federal and state authorities. Particularly at state level, it is beset by a range of procedural variations and specifications which are now optimised, at least in part, by means of a digital document exchange system. At present, however, IT solutions do not yet take full advantage of the digital support potential – not least because there is too little mutual ex-change.

One of the digital technologies that could reduce this fragmentation is blockchain (Christidis and Devetsikiotis 2016; Bonneau et al. 2015). Blockchain solutions facilitate a fully digital exchange of information among all members of the system, and this exchange is both fast and secure. Thus, everyone can instantly be made aware of the completion of essential steps within a given process, where-upon other authorities can immediately initiate follow-up steps accordingly (Fridgen et al. 2018b).

As part of a proof-of-concept (PoC), the Federal Office for Migration and Refugees (BAMF) has already tested the suitability of blockchain technology as a digital infrastructure for the coordination of federal administrative procedures (Fridgen et al. 2018a). Specifically, blockchain was used as a technology to support crossorganisational communication and cooperation in the asylum procedure. To this end, a simplified version of the asylum procedure was modelled on a blockchain basis. After a three-month implementation phase, the PoC was given a positive evaluation by experts of the Project Group Business & Information Systems Engineering at the Fraunhofer Institute for Applied Information Technology FIT.

Based on these results, the technology is now to be tested in a pilot project. This is to occur in the context of the AnkER Dresden facility and with the friendly support of Saxony's State Directorate (LDS). Previous communication channels between the Federal Office and the LDS have not been entirely effective, but rather beleaguered by various nondigital processes and the need for manual recording procedures. This has made them time-consuming and errorprone; two flaws which do not make for optimal processing. The use of blockchain shall now establish a timely and fully digital exchange of information within each sub-process, ensuring that the duration of procedures and the expenditure of resources can be significantly minimised, while security aspects can be considered more efficiently.

The Federal Office's pilot project thus occupies an important position in the wider administrative landscape, seeing as it serves as a lighthouse project that develops not only a concrete blockchain solution but also a series of transferable concepts. Meanwhile, prominent focus is placed on the implementation of data protection details and the

precise mapping of the current legal situation. With a view to this being a lighthouse project, the Federal Office will regularly publish its important findings (Fridgen et al. 2018a). This whitepaper reflects the findings made during the conception phase.

2. Essential background information

2.1 Order of Events in the asylum procedure in the AnkER-facility in Dresden

The asylum procedure in the context of AnkER-facilities does not differ significantly from the asylum procedure in general. For a detailed description of the German asylum procedure, please refer to the blockchain whitepaper of the PoC (Fridgen et al. 2018a) and the brochure of the Federal Office for Migration and Refugees (Bundesamt für Migration und Flüchtlinge 2016). The objective of AnkER-facilities is to provide a more efficient asylum procedure by bringing together under one roof the competent municipal, state, and federal authorities. Such local proximity of authorities and support staff shall ensure mutual exchange and smooth coordination of separate steps within the procedure.

AnkER-facility

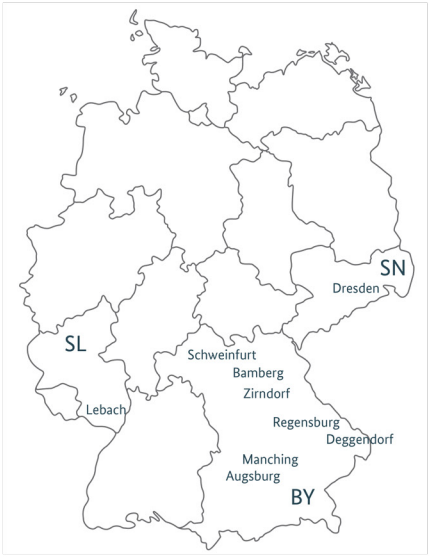
AnkER-facilities are of key significance not only in making asylum procedures more efficient, but also in ensuring that no time is lost when it comes to furnishing integration opportunities for those with a prospect of staying, or when it comes to beginning the return process quickly should an asylum application be denied.
(Dr. Hans-Eckhard Sommer, President of the Federal Office)

The acronym AnkER stands for Ankunfts-, Entscheidungs- und Rückkehreinrichtungen, which is german for the arrival, ruling, and return of asylum seekers. In AnkER-facilities, these tasks and areas of competence are all hosted in one place. The pilot phase started on 1 August 2018 with the opening of seven facilities in Bavaria (Augsburg, Bamberg, Deggendorf).

In August 2018, seven AnkER-facilities were launched in Bavaria, while a further one was set up in Saxony. In the pilot phase, which will continue until early 2020, predefined work procedures will be tested with regard to implementation and benefits. The procedures in question govern arrival, stay, and accommodation as well as complaint processing and integration initiatives, or otherwise return proceedings. The objective of AnkER-facilities is to ensure that applicants with a prospect of staying in Germany receive early integration opportunities such as language courses, vocational training, and guidance in everyday life, while the return process can also be accelerated, should an application have to be denied.

AnkER-facilities sit at the intersection of various areas of competence within municipal, state, and federal authorities. Thus, AnkER-facilities can involve several authorities alongside the Federal Office, such as the responsible foreigners' registration authorities, reception facilities of the respective federal state,

Facilities



Relevant Authorities

- Federal Office for Migration and Refugees
- Federal and state police
- Foreigners' registration offices
- Federal employment agency / job centres
- Administrative tribunals
- Social security offices
- Youth welfare services
- Public health authorities

Exemplary procedure

Integration

- Referral to an integration course
- Grading of language skills
- Test and registration office
- Communication of Germany's values an first orientation

Return

- Voluntary return or Repatriation
- Travel arrangements
- Counselling on return options

Asylum procedure & potential legal resources

- Complaint (Legal request office)
- Notification
- Decision
- Personal interview
- Asylum application

Arrival and registration

- Advisory service
- EASY-distribution
- Medical examination
- Identity verification
- Arrival

Figure 1: Exemplary procedure of an AnkER-facility

administrative tribunals, federal and regional police, youth welfare offices, public health departments, the Federal Employment Agency and other social authorities.

Responsibility for the AnkER-facilities rests with the respective federal state. Therefore, different federal states can set different priorities in their design of the asylum procedure. Figure 1 illustrates the commonalities and core functions of AnkER-facilities.

Compared to the general asylum procedure (Federal Office for Migration and Refugees 2019), the asylum procedure conducted in the context of AnkER-facilities has been slightly adapted or extended (Federal Office for Migration and Refugees 2018). The most important changes concern identity verification, counselling options with regard to application and return procedures, and inhouse opportunities to seek legal recourse. In the conventional asylum procedure, identity verification only takes place once the asylum application is processed. In AnkER-facilities, this stage of the process has been brought forward, meaning that a comprehensive identity check including verification of identity documents is now carried out during registration. In addition, an advisory service is now provided by the Federal Office. All asylum seekers are offered this service before they submit their application. This is done to inform them at an early stage about the asylum procedure as well as their rights and obligations. The asylum seeker can also receive counselling on various return options and return support programs, in particular when an application is denied. Depending on local circumstances, an administrative review of the asylum decision can be carried out via so-called legal request offices within the AnkER-facility. This makes for easier access to administrative courts and tribunals.

2.2 Blockchain

Blockchain is a transparent, transactional, distributed database structure that stores data in a decentralised, peer-to-peer network (Glaser 2017). By means of a so-called consensus mechanism, the network, rather than a central authority, determines the correct sequence of transactions in each block as well as the cryptographic and chronological concatenation of these blocks (Schweizer et al. 2017). Used in conjunction, the consensus mechanism and cryptographic procedures guarantee reliability, validity, security, and trust in the network (Christidis and Devetsikiotis 2016; Porru et al. 2017).

Which consensus mechanism is chosen depends, among other things, on the desired design of the blockchain network regarding its two key criteria, ‘participation’ and ‘authorisation’. In a public blockchain, participation in the network is open to everyone, whereas in a private blockchain, the group of participants is restricted. As for the issue of authorisation, there is a distinction between permissionless blockchains, in which all participants

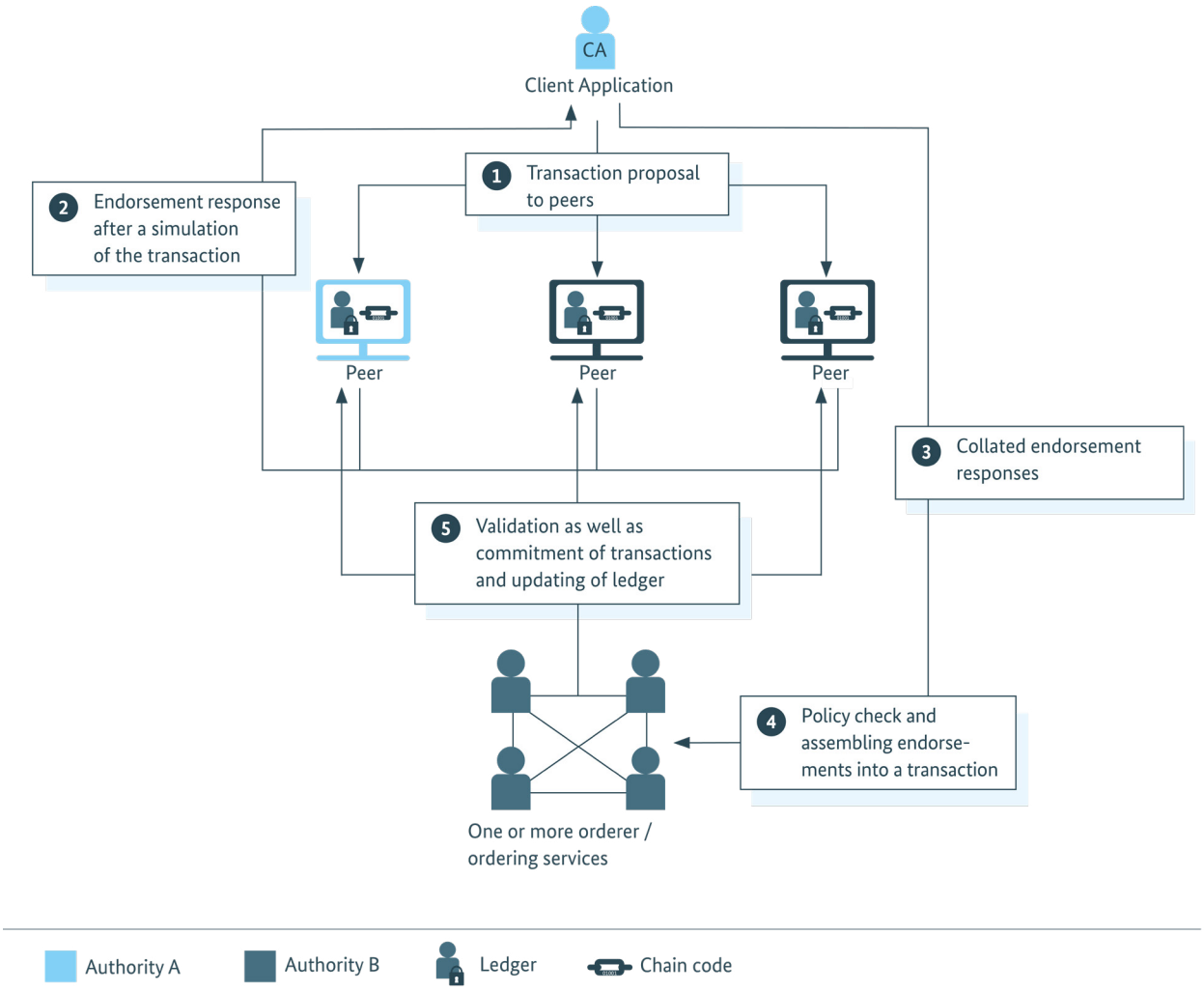


Figure 2: Transaction process via Hyperledger Fabric

are authorised to read and write, and permissioned blockchains, in which the rights of participants are controlled (Sajana et al. 2018; Androulaki et al. 2018). In private blockchain networks, limited access reduces the security burden placed on the consensus mechanism; for example, it is possible to choose a consensus mechanism by which members take random turns to confirm the validity of transactions. Such consensus mechanisms are associated with significantly higher transaction rates as well as lower resource consumption.

Aside from the design of a blockchain network and consensus mechanism, there are several further options for differentiation, such as the type of cryptographic link. Additionally, most blockchain technologies offer the possibility of mapping process logics by way of so-called smart contracts and executing them automatically whenever predefined trigger points are encountered. There is, then, no 'one' type of blockchain.

Accordingly, the Federal Office has performed a comprehensive analysis of existing blockchain technologies, with a particular focus on Ethereum and Hyperledger Fabric. In the end, Hyperledger Fabric was chosen since it was specifically designed for organisational use.

Hyperledger Fabric is one of the Hyperledger projects currently under development by the Linux Foundation (Linux Foundation 2017). Unlike the Bitcoin blockchain and Ethereum, Hyperledger Fabric uses a private and permissioned design.

Specifically, Hyperledger Fabric has a modular and flexible structure which supports easy adaptation of individual components to the requirements of the application. It also supports targeted expansion to include new approaches and technological possibilities. In addition, Hyperledger Fabric is well scalable (Linux Foundation 2017; Osterland and Rose 2018) and the fact that it is anchored in the Linux Foundation promises reliable longterm development. What is more, Hyperledger Fabric can easily be operated on various physical and virtual infrastructures, and it supports a range of programming languages that can be used to implement smart contracts (Sajana et al. 2018; Linux Foundation 2017; Androulaki et al. 2018).

The precise function of the Hyperledger Fabric is based on three different roles within the network: client, peer, and orderer, although the peer role can be further differentiated into endorser and committer (Linux Foundation 2017). The client creates transactions on behalf of the end user, then submits them to endorsers for verification. Endorsers simulate the transactions and give the client feedback on their validity. They also give the client a read/write set. Subsequently, the client forwards the verified transaction proposals to orderers (also known as ordering services), who perform a syntactical verification in line with the endorsement policy and then group transactions into blocks. The finished blocks are sent back to the peers or, more specifically, to the committers. In the final instance, then, the orderer ensures that all peers receive the same transactions in exactly the same logical order. The committers run checks to safeguard that all previous steps in the consensus mechanism were executed correctly and that no changes made to the blockchain in the meantime have rendered the transactions invalid. Only then are the new blocks added to the blockchain (Le Hors et al. 2018). As a rule, all transactions are included in the blockchain, but invalid transactions are flagged. Figure 2 illustrates the transaction flow of a Hyperledger Fabric.

3. Blockchain pilot in the AnkER–facility in Dresden

3.1 Objectives of the pilot project

The overriding objective of the blockchain pilot project is to develop a functional blockchain solution and run it in a field test. Specifically, answers are sought to questions of acceptance and cost-effectiveness as well as potential and technical optimisation. Apart from these strategic and technical objectives, the non-objectives of the pilot project are also clearly defined.

Strategic objectives

1. The pilot project is to make a significant contribution to knowledge advancement and cross-organisational exchange on the possible applications of blockchain technology in the area of public administration in Germany.
2. The pilot project is to shed light on whether blockchain technology can be put to a sensible use in the public sector while staying within the bounds of the coalition agreement.
3. In the event of a positive evaluation, the pilot project is to provide well-founded proposals on how to set a standard for the use of blockchain technologies in other authorities.

Technical objectives

1. The blockchain solution is to increase the transparency, productivity, and efficiency of cooperation between Saxony's State Directorate and the Federal Office in the AnkER-facility Dresden. Most notably, there is great potential in their ability to establish a shared and persistent level of information, to do so across organisational boundaries, and to do so quickly and securely. Overcoming trust barriers, on the other hand, is of little importance in the asylum procedure.
2. The blockchain solution is to serve as a preventative measure by cautioning against deviations from the standard procedure of the AnkER-facility Dresden. If necessary, it is to record these incidents.
3. The blockchain solution is to accelerate the processing of selected stages in the asylum procedure.
4. There is to be an increase in the quality of information with regard to rulings on asylum applications. Also to be raised is legal compliance when registrations and case details are processed.

Non-objectives

1. This blockchain solution is to replace the preexisting systems of the Federal Office and the LDS.

2. Once implemented, this blockchain solution is not to be used for electronic performance monitoring, nor is it to allow access to mass data.

3.2 Supported sub-processes

In this pilot project, three sub-processes are supported by the blockchain solution: 'registration, creation of an application file, and personal interview', 'referral', and 'ruling and next steps'. These sub-processes were selected because they require close cooperation and coordination between the Federal Office and the LDS.

In all three sub-processes, only those activities of the Federal Office and LDS are evaluated. The involvement of other authorities (e.g. the part played by the health office during the registration process) is not part of the pilot project.

The sub-process 'registration, creation of an application file, and personal interview' can be further subdivided into nine stages. Figure 3 illustrates each of these stages as well as the individual parts of the process that are to be evaluated by the Federal Office and LDS.

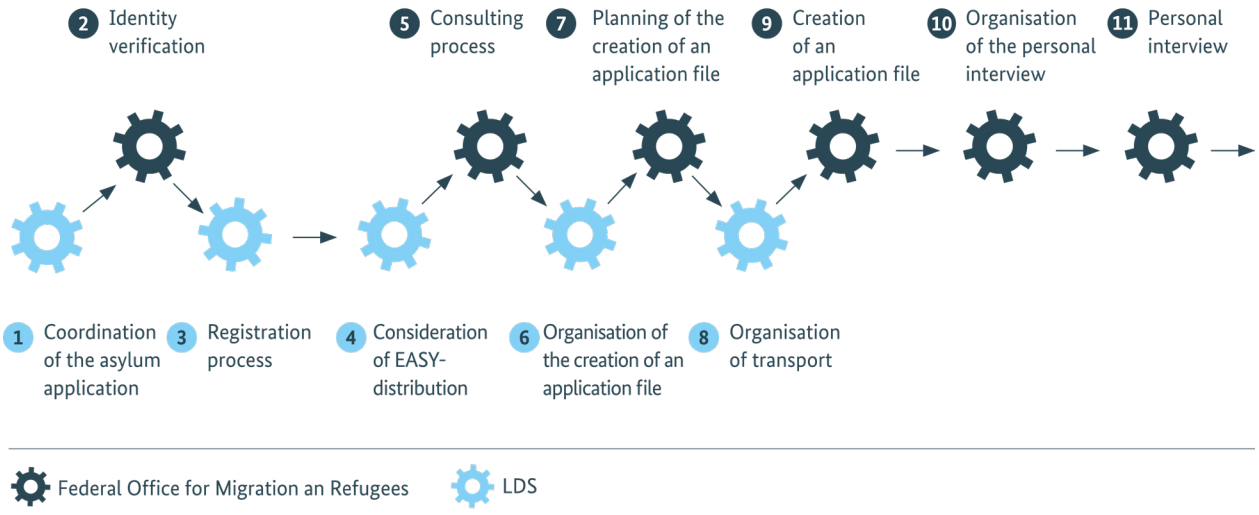


Figure 3: Sub-process 'registration, creation of an application file and personal interview'

In the sub-process 'referral', there is a distinction between two possible scenarios: 'good prospect of staying' and 'Dublin procedure'. Figure 4 shows the scenario 'good prospect of staying'. If there is a positive ruling, i.e. a good prospect of staying, then this scenario is subdivided by areas of competence into six process steps.

Figure 5, on the other hand, illustrates the alternative referral scenario, which calls for the 'Dublin procedure'. This procedure determines which member state of the European Union is responsible for the processing of an asylum application. If the review of the Dublin Centre concludes that a different member state could be responsible for processing an asylum application, a so-called transfer request is sent to the respective member state. If said member state consents to this request, the Federal Office will rule that the asylum application is in-admissible in Germany, whereupon the applicant will be referred to the other member state to seek asylum there. Should the applicant not comply with this departure request, the Federal Office will issue a deportation order. If, however, the 'Dublin procedure' is not performed, or if it is aborted, then the asylum seeker may opt for reapplication elsewhere in Germany, as illustrated in the sub-process 'referral'.

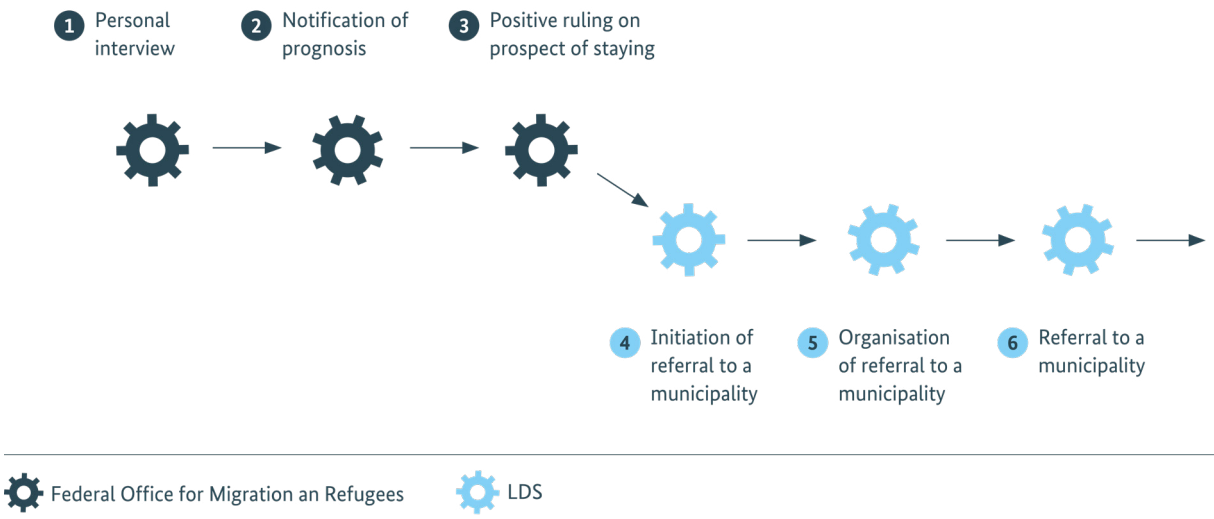


Figure 4: Sub-process 'referral' - scenario 'good prospect of staying

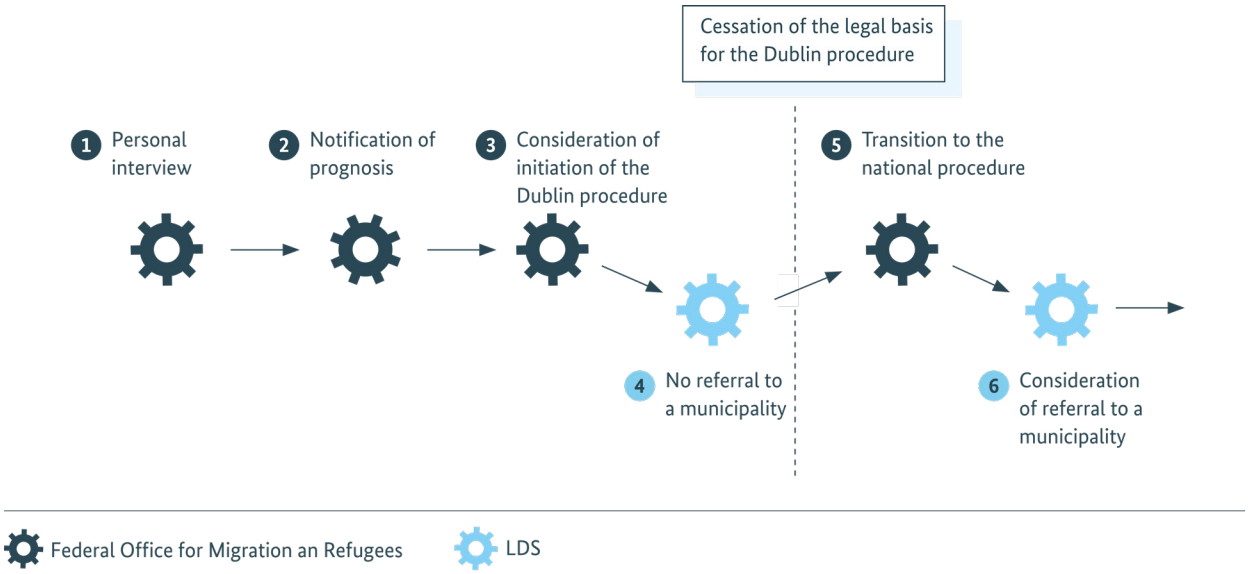


Figure 5: Sub-process 'referral' - scenario 'Dublin procedure'

The sub-process 'ruling and next steps', illustrated in figure 6, can be subdivided into five or indeed six process steps, depending on the ruling reached in the respective asylum application. However, not in every case will an application necessarily go through all of these process steps.

3.3 Challenges of data protection laws

The General Data Protection Regulation (GDPR) came into force on the 25th of May 2018. The GDPR applies uniform regulation to the protection and processing of personal data by private companies and public bodies (data processing bodies) in the European Union. In addition to general rules and regulations for the storage and automatic processing of personal data, the GDPR also strengthens the rights of the person concerned, that is the data subject (Chapter 3, Articles 12-23 GDPR). These rights include the right to rectification (Article 16 GDPR) and the right to erasure ('right to be forgotten') (Article 17 GDPR). The right to rectification also stipulates that the data controller must rectify incorrect, out-of-date, or incomplete personal data without delay. According to the right of erasure, the party concerned may request the deletion of their personal data if the retention of said data is no longer necessary for the purpose for which it was originally collected, or if the data was unlawfully processed, or if the party concerned has withdrawn their consent for further retention. A special case for an erasure

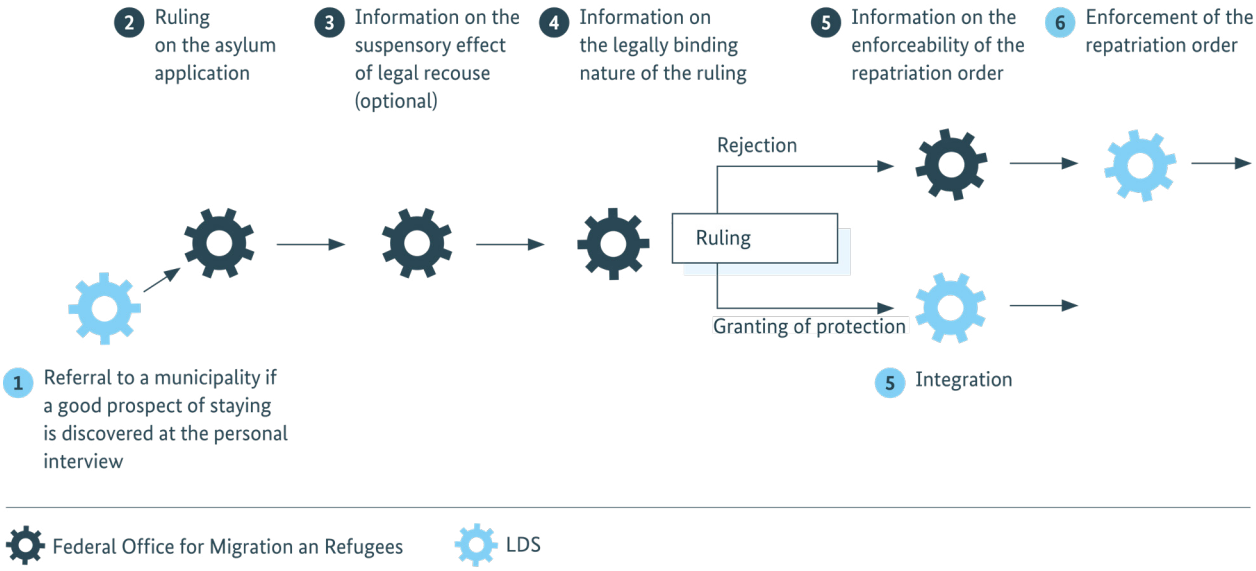


Figure 6: Sub-process 'ruling and next steps'

claim is the 'right to be forgotten'. This right applies when data has been published, and it is of special relevance with regard to publications on the Internet.

However, compliance with the rights of data subjects enshrined in the GDPR places certain limits on the technical application of blockchain. First of all, due to the 'hashing' of blocks, blockchain solutions are considered to be unchangeable and, above all else, non-erasable. This creates certain challenges with regard to the right to rectification and the right to erasure. Furthermore, according to the GDPR, it has to be clearly defined who assumes responsibility for ensuring compliance with the GDPR. This is of particular importance when several parties have joint control over the processing of personal data, as is generally the case in decentralised systems, and indeed in blockchain networks. To this end, arrangements must be created among the parties to regulate the transparent delegation of responsibilities and duties.

Since the remit of the GDPR extends to administration, the pilot project includes the development of an architecture along with a rectification and erasure concept which, according to the current view of the Federal Office, conform to data protection regulations. The architecture as well as the rectification and erasure concept also ensure compliance with the rights of data subjects, as stipulated in chapters 16 and 17 of the GDPR. Further details on this can be found in chapter 4 of this whitepaper.

4. Essential concepts for real-life operation

4.1 System architecture

The architecture of the blockchain solution is divided into three layers (see Figure 7). Located on the lowest layer, the back-end layer, are the existing workflow management systems and data repositories of the respective authorities. Above this is the integration layer, which hosts a dashboard layer in which content from the backend layer and the blockchain layer can be displayed, depending on the role and access rights of the authority. In addition, the integration layer includes the so-called privacy service layer, which enables a data protection-friendly mapping not only of unique, pseudonymised reference characteristics on the blockchain but also of technical characteristics in the back-end systems. The ways in which the dashboard and privacy service layer are integrated may differ between authorities. The technical design of the system, however, must comply with general parameters that apply to all authorities.

Only the third level, where process updates can be shared via the blockchain, is uniformly designed with regard to both integration and technical design. The blockchain connects the various existing workflow management systems and data repositories to form a network in which information can be securely shared. The blockchain layer thus serves as a 'technological and IT bracket' placed around the various back-end layer systems.

The interfaces between the privacy service layer and the blockchain layer are standardised and secure. This facilitates comparatively simple scaling, since the dashboard and privacy service layer can be designed according to the requirements of a new authority and connected to the blockchain via a standard interface.

Blockchain layer

The blockchain layer comprises a private, permissioned blockchain based on Hyperledger Fabric. For reasons of simplicity during this pilot project, the current plan is for the blockchain nodes to be hosted and operated in a multitenant cloud environment of the Federal Office. Consensus will be reached on the basis of a common consensus algorithm that is yet to be determined. However, the consensus algorithm can subsequently be replaced due to the modular structure of Hyperledger Fabric.

In order to implement the requirements of the GDPR, particularly the right to erasure, no personal data is stored on the blockchain. Indeed, the current plan is for there to be no other data stored on the blockchain for each process update other than the individual asylum applicazion's unique, pseudonymised attribution characteristic (blockchain ID), the current process status, the timestamp, and the ID of the competent authority.

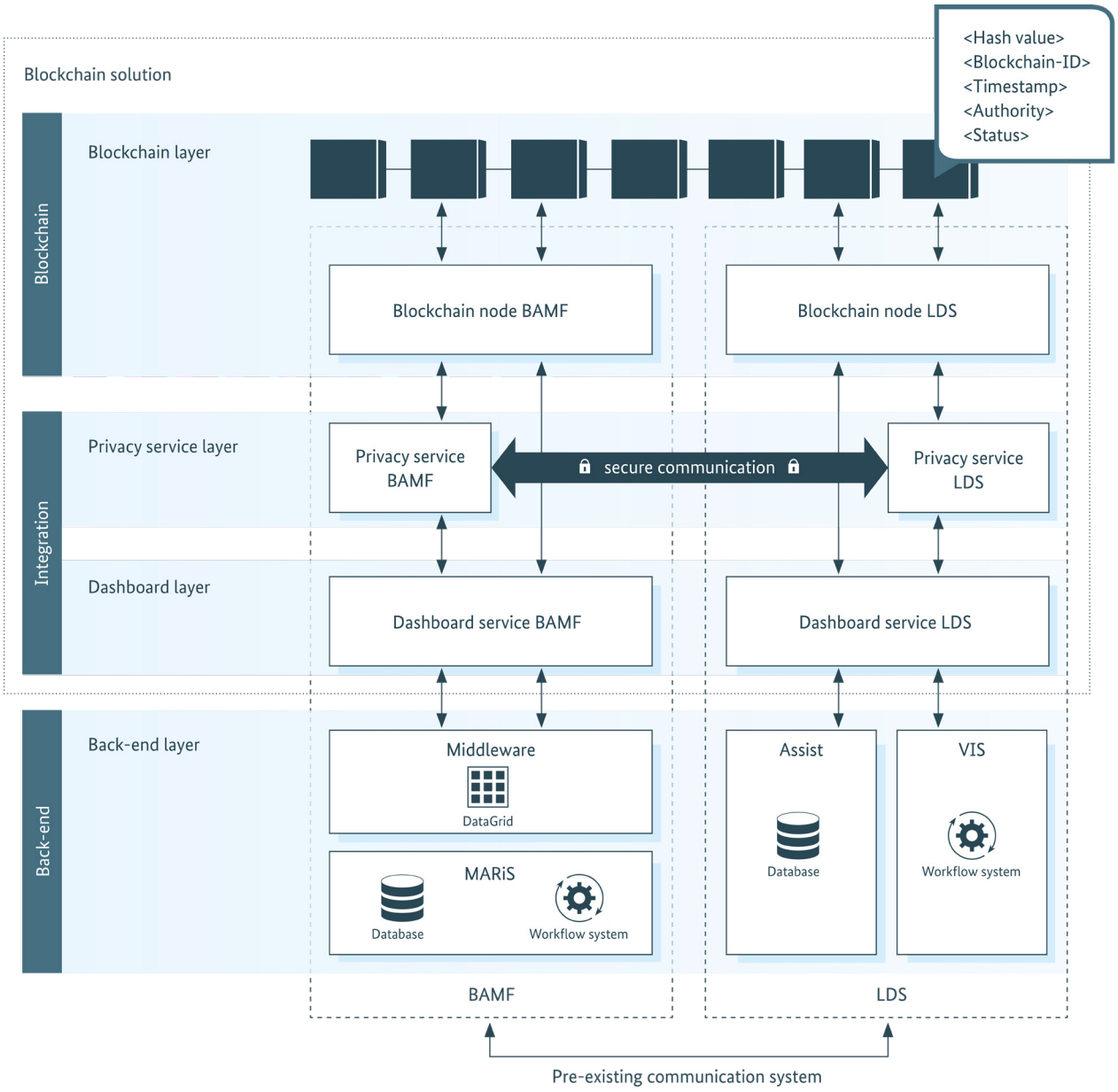


Figure 7: Illustration of the system architecture

Integration layer: Privacy service layer

The main function of the privacy services consists in the attribution of blockchain IDs to the IDs used by the respective authorities (e.g. in the form of file numbers). This attribution is to be in compliance with data protection laws, i.e. deleteable and changeable. Without such an attribution, the status updates on the blockchain have no usable information content.

While it is possible to see on the blockchain level which specific process updates belong to a blockchain ID, it is not possible for any authorities or other third parties to link these to a specific asylum procedure, nor to a specific applicant, without knowing the respective attribution in the privacy services.

To put it in slightly more technical terms, the privacy services are designed as highly secure mapping services that support role-based access procedures for different user groups and can create, change, and delete the mapping between authority-specific and blockchain IDs.

The privacy services also offer authorities the option to exchange attribution information with end-to-end encryption via a pre-existing off-chain channel. This form of exchange is particularly important the first time the responsibility for an asylum procedure is transferred to another authority, because it prevents an application from being recorded on the blockchain several times, all with different blockchain IDs.

DataGrid

The DataGrid constitutes a secure inquiry service. It facilitates decoupling from the various back-end systems of the Federal Office. It also offers each user a customisable storage and provision of data from those back-end systems.

Integration layer: Dashboard layer

To illustrate the current status of asylum applications, a dashboard-based system that can be used via a web browser was developed. Depending on the access rights of a user, all content with relevance to the performance of a respective task is displayed here. Via standardised and secure interfaces, this layer is linked to the privacy service layer as well as to the back-end system layer. Hence, these interfaces make it possible not only to find out about the status from the blockchain by way of mapping, but also to load further data directly from the back-end system, depending on what the user is authorised to access.

Back-end layer

In accordance with federal legislation, each authority continues to manage its existing workflow management systems and data repositories independently. At the Federal Office, these systems comprise middleware services along with the central workflow and document management system MARiS, which in addition to data management also offers workflow management functions. The connection between the dashboard layer and the back-end layer of the Federal Office is established via so-called middleware services provided by the Federal Office. These middleware services include the so-called DataGrid.

The back-end systems of the LDS consist of a procedure support system, ASSIST, including various databases and a workflow management system, VIS. All personal and sensitive data will continue to be stored decentrally in these back-end systems. Push-based transmissions of this data can be reduced, since other authorities can instead request it pull-based, if an inquiry is justified. Each of these requests will then necessitate an (automated) identity and authorisation check.

Evaluation of the architecture

The decision to keep sensitive data in the back-end systems takes account of the federal structure of the asylum procedure, but it also makes a substantial contribution towards the consistent implementation of the once-only principle, since it prevents redundant storage of personal data by various authorities. As well as that, the architecture can safeguard the rights to rectification and erasure (Articles 16 and 17 GDPR). This will be explained in detail in the following chapter.

What gives this system architecture its special value is the fact that operative procedural data can be shared between different authorities via the blockchain, that this can be done in accordance with current legal stipulations (e.g. GDPR), and that it can be done without losing data sovereignty or having to store personal data directly on the blockchain.

4.2 Erasure and rectification

The right to erasure (article 17 GDPR) stipulates that personal data must be erased if the purpose for which it was collected no longer exists. In the context of the asylum procedure, this is the case when, for instance, the asylum procedure has been completed. Furthermore, the Asylum Act stipulates that data must be deleted no later than ten years after the asylum procedure has been completed (article 7, paragraph 3 Asylum Law).

The erasure of data affects all three layers of the blockchain solution developed by the Federal Office. An illustration of the erasure process is shown in Figure 8.

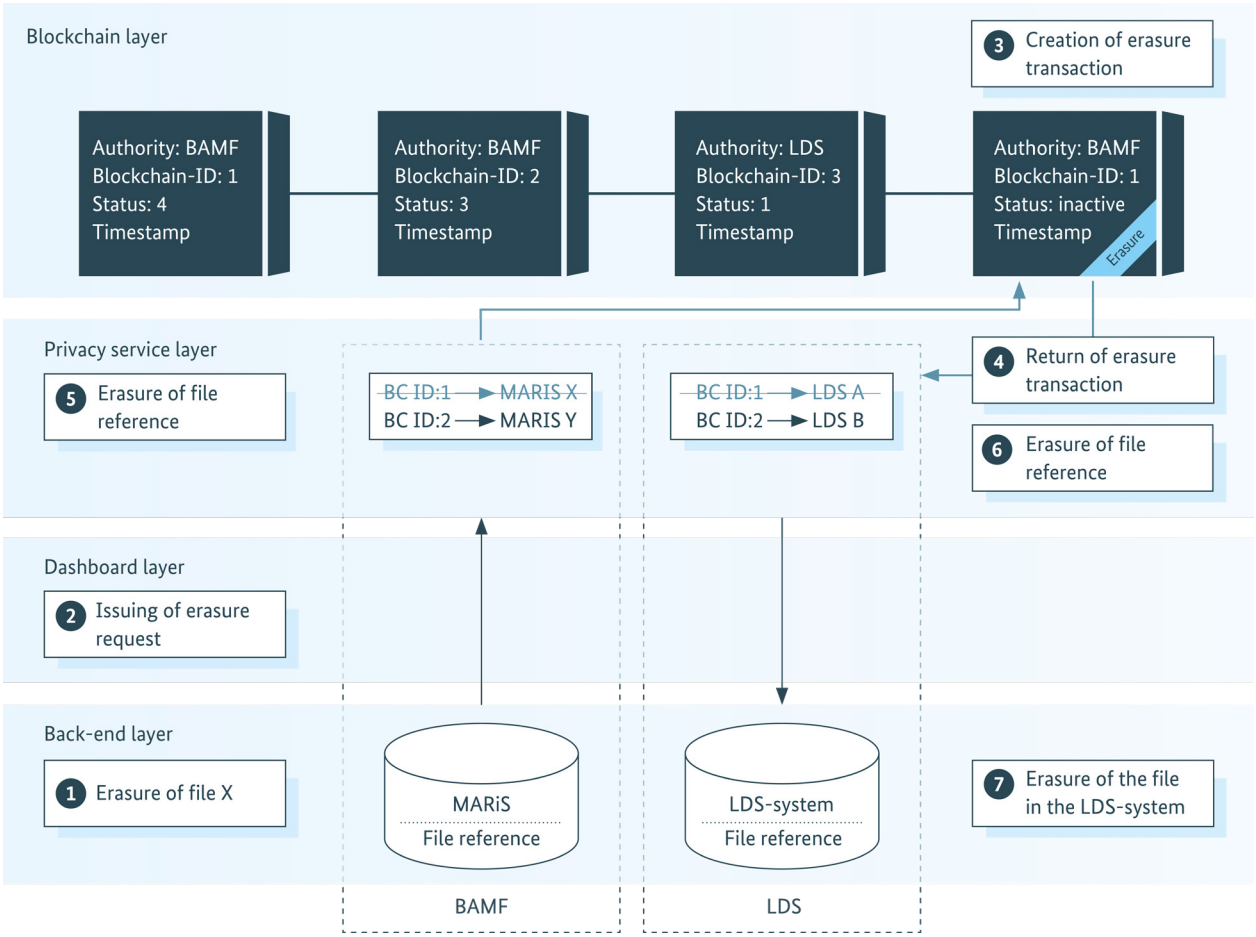


Figure 8: Erasure of data from the blockchain solution

First of all, the data in question is deleted as per usual in the authority's back-end systems (step 1). Subsequently, a notification of the erasure process is sent to the authority-specific privacy service (step 2), which in turn stores a so-called 'erasure transaction' on the blockchain (step 3).

This erasure transaction makes it apparent that the information belonging to a particular asylum procedure, filed under the respective blockchain ID, has been deleted in the authority's back-end systems, and that the blockchain ID is no longer to be used. The other authorities participating in the

blockchain network are informed of the erasure via the blockchain (step 4). Finally, the authority that issued the erasure transaction now deletes the file reference in its privacy service (step 5). With that, all corresponding file references in the privacy services of the other authorities (of the LDS in Figure 8) are automatically deleted (step 6).

The erasure of relevant data in the back-end systems of other authorities (step 7) remains the sole responsibility of the respective authorities. It is not monitored via the blockchain. It would be conceivable that all other authorities which have reacted to the erasure transaction by deleting the corresponding data in their back-end systems also document this with a transaction in the blockchain, but no authority shall be obliged to delete data from its back-end systems due to the blockchain solution.

However, if there is a legal obligation to delete, and if all authorities comply with this obligation and remove the corresponding data from their systems, only the status report stored on the blockchain remains. Since the file reference in the privacy services has also been deleted, the respective authority can no longer link the blockchain ID to a specific request. Due to the algorithm used, it is no longer or only with disproportionate effort possible to attribute the status report on the blockchain to an application.

With further regard to compliance with data protection, the rectification of false data on the blockchain (article 17 GDPR) is as important as the ability to delete it. Even when the asylum procedure is overseen in an AnkER-facility, it may for various reasons be necessary to rectify information stored on the blockchain. This is the case, for example, when employees accidentally enter incorrect data and a wrong status is written into the blockchain or status reports have to be revoked due to external influences.

In this process, the rectification is first made in the back-end systems (step 1), whereupon the rectification is reported to the privacy service (step 2). The privacy service now creates a new, so-called rectification transaction on the blockchain (step 3). This update makes it apparent which status is to be changed and determines the status that is now valid. The blockchain informs the other authorities participating in the blockchain network about the rectification, which enables them to process said rectification (step 4). For example, follow-up processes that have already been started can now be stopped and, if necessary, reversed (step 5). This can prevent unlawful repatriations for which there is no legal basis due to appeals lodged on short notice. An illustration of a rectification process is shown in figure 9.

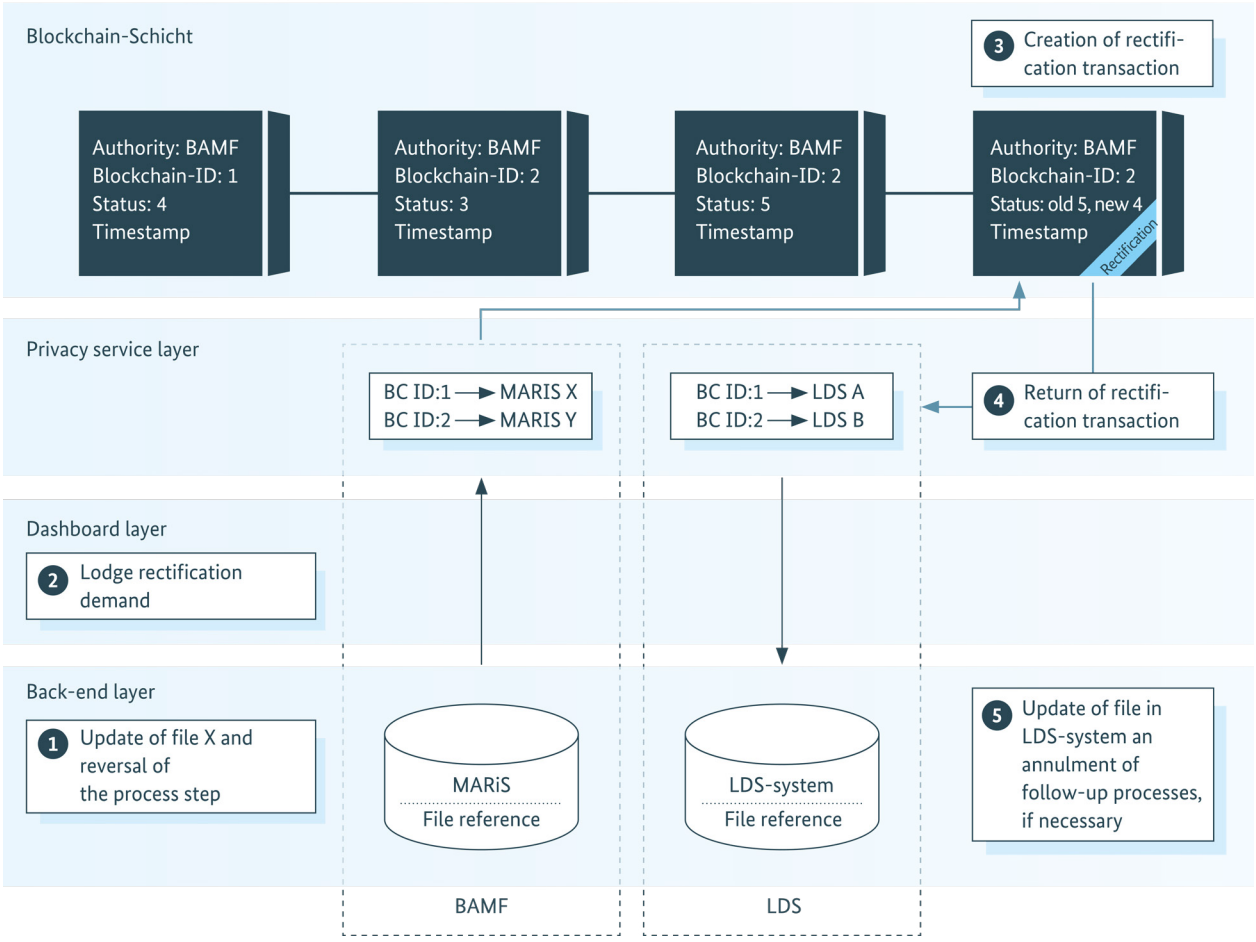


Figure 9: Rectification of data in the blockchain solution

4.3 Governance

The use of a blockchain solution requires coordination at several levels. This starts with the definition of functional requirements and extends to the delegation of tasks in the operative procedure. In order to minimise the complexity of the necessary coordination, there is a need for an effective delegation of decision-making competencies and responsibilities, i.e. effective governance. Specifically, such a delegation is important at the technical, organisational, and data protection level.

Governance regarding data protection laws

The development of a blockchain solution poses a number of data protection challenges. Especially important is a transparent delegation of responsibilities for compliance with the requirements of the GDPR.

Technical governance

At the technical level, too, effective governance structures must be created and methods used to ensure the smooth development and reliable operation of the blockchain solution.
In the development phase, the blockchain solution must be adapted to the technical requirements of all parties involved. This depends on close coordination among the respective IT departments. By way of technical governance structures, a delegation of responsibilities and implementation competencies has to be defined and ensured to be sustainable. It is also necessary to put this delegation into concrete terms by means of a development model that corresponds to the desired design of the blockchain.

Another aspect of technical governance is dealing with the operational questions about the blockchain layer and the underlying software and hardware layers. In general, the parties involved should be left to answer those questions for themselves. However, a blockchain solution is only as functional and secure as its weakest link. Therefore, the selection of potential operating models and their operators should be predicated on certain minimum requirements.

Organisational governance

When it comes to the organisational governance of a blockchain solution, it is of paramount importance to ensure that both the general and the functional requirements of the parties involved are reliably incorporated into the development of the system. One of the general requirements in public administration in Germany, for example, is the consideration of the federal framework.

Governance in the pilot project

To run this pilot project in the context of the AnkER-facility Dresden, an agreement on joint responsibility for compliance with the requirements of the GDPR is currently being drawn up between the Federal Office and the LDS. To keep things simple during the pilot phase, the blockchain solution will be developed and supplied by a joint provider. In the subsequent real-life operation, however, the various authorities can choose different providers. To this end, minimum requirements for the on-boarding of other operators are to be worked out in the further course of the project. As for the organisational dimension of the pilot project, there will be several rounds of mutual review and joint decision-making with regard to both the general and the specific functional requirements.

4.4 Scalability

To keep the project's complexity in the pilot phase to a minimum, only two authorities are connected to the blockchain solution. However, a special focus was placed on scalability in order to accommodate other authorities and multiple variations of the asylum procedure.

With this in mind, the Federal Office has performed an in-depth evaluation of other blockchain solutions being developed in Germany and Europe. A project that offers an especially promising opportunity to tie in with our own is the planned 'European Blockchain Services Infrastructure', the development of which has been actively promoted by the 'European Blockchain Partnership' (EBP) since 2018. The aim of this European initiative is to create a blockchain infrastructure for public administration in Europe. This infrastructure will provide various services and allow for various applications to be implemented. At this point in time, however, the EBP does not yet provide any specifications and recommendations. The blockchain solution of the Federal Office is thus based on best practices of successful projects in the private sector.

In specific terms, these best practices extend to the areas of data protection, technology, and organisational design, much like in the case of the governance concept.

Data protection scalability

In accordance with the GDPR, a single authority must be placed in charge of the processing and storage of data. Alternatively, this role can be assumed by several or indeed all authorities together (joint control). In the latter case, an arrangement must be created which regulates the details of joint responsibility.

In real-life operation with a large number of authorities, however, joint responsibility by all authorities cannot be made to work in a sensible way. Nevertheless, it will likely be necessary for

certain select authorities (including the Federal Office) to assume joint responsibility. Accordingly, the agreement between the Federal Office and the LDS will be role-based and expandable in order to allow for the addition of further authorities in different roles.

Technical scalability

To ensure technical scalability, it has to be possible to connect further authorities with ease. The blockchain solution thus relies on the development of a reference architecture consisting of standard interfaces, common technologies, and a data model that offers flexible expansion. The responsibility to integrate the blockchain solution with its back-end systems lies with the new authority. Each authority can decide for itself which of the data stored in the blockchain it wants to process and how it wants to do so (e.g. individual warning functions regarding process deviations). As a result, the complexity of the blockchain remains manageable – even with a very large number of authorities.

What is more, the blockchain solution accommodates different hosting models and enables authorities without prior knowledge of blockchain technology to connect quickly via standard configurations.

Organisational scalability

Organisational scalability covers two essential aspects. On the one hand, safeguards have to be put in place to ensure that the requirements of other authorities (e.g. security authorities) can be met. On the other hand, further safeguards are necessary to ensure that new authorities are given the opportunity to participate in shaping the overall process, yet do so without creating any substantial loss of agility in the decision-making process.

Here, as in the above section on data protection scalability, the Federal Office opts for small working groups in which a select few of the participating authorities represent the interests of the wider network.

5. Design principles for blockchain solutions in public administration

During the conceptualisation phase, the Federal Office laid important foundations for the design of blockchain solutions that are compliant with data protection laws and meet the requirements of public administration. This was necessary because there are, to date, no best practices, nor indeed any precedents on how to implement a blockchain solution for Germany's administrative procedures. In particular, no past experience is available to indicate the extent to which blockchain-inherent properties, such as non-erasability, can be brought into compliance with the GDPR.

The experience and findings of the Federal Office, meanwhile, can be summarised in four basic design principles.

Design principle 1: Personal data should not be stored on the blockchain.

Storing personal data on the blockchain is to be avoided. Personal data is to remain in the back-end systems of the respective authority.

According to the assessment of the Federal Office, this principle should also apply to all hash values that refer to personal data, since advances in computing power could ultimately make old hash functions reversible with manageable effort.

Of further critical significance are specific references on the blockchain. As soon as data stored on the blockchain can be used to identify an individual person, it constitutes personal data and is thus subject to the GDPR. Accordingly, the data on the blockchain should be kept to a minimum, and existing IDs should not be used in the blockchain.

Design principle 2: Should a use case make it necessary that data on the blockchain is attributed to an individual person, a highly secure off-chain mapping architecture is to be used.

Certain use cases, such as those of the Federal Office, make it necessary that information stored on the blockchain can be attributed to an asylum application, should circumstances require it. It follows that the information can then also be linked to an individual person, namely the asylum seeker or applicant. Since design principle 1 also applies in these cases, the information on the blockchain must not be designed in such a way that an individual person can be identified without additional information.

To this end, a pseudonymisation solution is to be used. Here it is advisable to use a mapping solution that links pseudonymous reference characteristics

on the blockchain with the specific reference characteristics used by the respective authorities. These mapping solutions are to be designed off-chain, and they are to exchange mapping information exclusively via secure information channels.

By means of such mapping solutions, data managers can comply with the right to rectification and erasure by 'rectifying' the data through rectification transactions, and by deleting the mapping, they can depersonalise the data on the blockchain from their subjective perspective, i.e. 'delete' it.

Design principle 3: Blockchain should be considered as a component of an overall solution to improve communication and collaboration.

Blockchain solutions should not be designed as detached systems. By delegating process updates to all members of the blockchain network, a blockchain solution can instead provide an overall solution that improves communication and collaboration. To be specific, a blockchain solution can facilitate both pull- and push-based data exchange. In a pull-based exchange, an authority that detects a relevant process update elsewhere can contact the issuing authority for further information. The issuing authority can then check such requests individually, document this process and accept or reject each request, depending on whether it is legitimate. If it is legitimate, the issuing authority can respond through information channels that have been established as secure with end-to-end encryption. In a push-based exchange, meanwhile, the issuing authority sends the process update and, if necessary, the relevant information to all authorities affected by this update. In order for the exchange between authorities to function smoothly, all authorities in the blockchain network must agree on which standards shall apply to their data exchange.

Design principle 4: The blockchain is to be implemented as a separate, modular system layer.

A blockchain is not to be used to perform functions which could be better performed by proven solutions such as central databases. Blockchain is not a good choice when an application requires a single, easily accessible data-base for large amounts of data that can be updated in close to real-time. It is also difficult to use blockchain to support processes that are currently more effectively supported by established workflow management systems. Instead, blockchain is a solution intended for distributing and securing process updates among organisations when the context does not allow for central control of the workflow. In other words:

Blockchain solutions should play a complementary role in a collaborative, cross-organisational context.

In such cases, blockchain facilitates a more effective information exchange between fragmented data repositories.

To this end, the design of the blockchain solution should include loosely coupled components, standardised interfaces, and a data model with the potential for flexible expansion. These elements facilitate efficient maintenance, continuing development, and – if necessary – they make it possible to replace the blockchain level at a later point in time. They also enforce abstraction from the blockchain protocol and enable other organisations to connect to the blockchain network with ease.

6. Future prospects

The pilot project is currently in the development phase, which is to be completed by the end of 2019. In this phase, the concepts presented in this whitepaper will be implemented. At the beginning of next year, the project will enter a three-month trial and evaluation phase in limited real-live operation. In order to evaluate the specific advantages of a blockchain solution, there will be an exhaustive and comprehensive examination of the changes that will have occurred in the asylum procedure in the context of the AnkER-facility Dresden. The general purpose of this is to evaluate whether blockchain technology is suitable to the project's intended purpose and to what extent it has served this purpose. All data will be collected in a methodical manner, analysed in full, and documented in such a way as to make the procedure, the evaluation, and the results understandable as well as verifiable. The evaluation works by way of comparison, taking into account the values identified before (ex-ante values) and after (ex-post values) the introduction of the blockchain solution.

The Federal Office is expecting to identify improvements with regard to transparency, efficiency, integrity, and communication in the cross-organisational collaboration in the context of AnkER-facilities. These advantages would further increase significantly with every additional authority that can be connected to the blockchain solution. What is more, the Federal Office expects the pilot project to produce insights which will point the way towards significant improvements in the decentralised design of cross-organisational IT systems. Unlike centralised systems, such decentralised cross-organisational systems are better suited to Germany's subsidiary and federal organisational structures and could thus make a fundamental contribution to the digitisation and networking of municipal, state, and federal authorities. Accordingly, this pilot project plays a pioneering role among the IT projects currently run by federal authorities in Germany.

If this pilot project has the anticipated success, various expansion scenarios for the blockchain solution are conceivable. For instance, AnkER-facilities could take it upon themselves to further subdivide current stages of the asylum procedure or include additional stages (such as the process of cancelling and withdrawing protection). Another expansion option is the inclusion of further authorities in the asylum procedure. To this end, further AnkER-facilities or authorities with similar functions should be brought on board, be it in Saxony or in other federal states of Germany. Another possibility is to use the blockchain solution for other purposes (such as the integration process) or indeed in entirely different contexts in which the concepts and design principles developed in this pilot project can serve as a blueprint and guideline.

At the same time, it should be noted that different use cases or contexts can place different requirements on the design of the blockchain solution, which is why a 'one-size-fits-all' solution is not advisable and adaptations may have to be made. These different blockchain solutions should, however, be combinable with each other to ensure that an

infrastructure of various blockchain solutions can be created. Based on this infrastructure, a Europe-wide solution is conceivable in addition to a Germany-wide solution. In such a scenario, the asylum authorities of all EU states could, for example, handle the Dublin procedure much more transparently and efficiently via a common blockchain infrastructure – without having to transfer sovereignty over national data to a central server at EU level.

Due to the federal structures within Germany and Europe, however, this infrastructure would have to be designed in such a way as to reflect the respective structures and associated challenges with regard to individual responsibilities and procedural variations, and indeed in accordance with current law. In the asylum context, blockchain could thus become the ‘digital enabler’ of European federalism and constitute a further step towards a united Europe.

7. References

Androulaki, Elli; Manevich, Yacov; Muralidharan, Srinivasan; Murthy, Chet; Nguyen, Binh; Sethi, Ma-nish et al. (2018): Hyperledger fabric. In: Pascal Felber, Y. Charlie Hu und Rui Oliveira (Hg.): Proceedings of the Thirteenth EuroSys Conference on EuroSys ,18. the Thirteenth EuroSys Conference. Porto, Portugal. New York, New York, USA: ACM Press, S. 1–15.

Bonneau, Joseph; Miller, Andrew; Clark, Jeremy; Narayanan, Arvind; Kroll Joshua A.; Fel-ten, Edward W. (2015): Sok. Research perspectives and challenges for bitcoin and crypto-currencies. In: IEEE Symposium on Security and Privacy, S. 104–121.

Federal Office for Migration and Refugees (2016): Stages of the German asylum procedure. An overview of the individual procedural steps and legal framework. In cooperation with Saliha Kubilay. Edited by the Federal Office for Migration and Refugees, published by the Federal Office for Migration and Refugees. Available online: https://www.bamf.de/SharedDocs/Anlagen/DE/Publikationen/Broschueren/das-deutsche-asylverfahren.pdf?__blob=publicationFile, last checked: 11.04.2019.

Federal Office for Migration and Refugees (2018): AnkER-Facility – An Overview. Available online: http://www.bamf.de/SharedDocs/Anlagen/DE/Downloads/Infothek/DasBAMF/ankereinrichtungen-ueberblick.pdf?__blob=publicationFile, last checked: 11.04.2019.

Christidis, Konstantinos; Devetsikiotis, Michael (2016): Blockchains and Smart Contracts for the Internet of Things. In: IEEE Access 4, S. 2292–2303.

Fridgen, Gilbert; Guggenmos, Florian; Lockl, Jannik; Rieger, Alexander; Urbach, Nils (2018a): Support of communication and cooperation in the asylum procedure with the help of blockchain. Available online: http://www.bamf.de/SharedDocs/Anlagen/DE/Downloads/Infothek/DasBAMF/blockchain-whitepaper.pdf?__blob=publicationFile, last checked: 11.04.2019.

Fridgen, Gilbert; Radszuwill, Sven; Urbach, Nils; Utz, Lena (2018b): Cross-Organizational Workflow Management Using Blockchain Technology – Towards Applicability, Auditability, and Automation. In: Proccedings of the 51th Hawaii International Conference on System Sciences, S. 1147–1156.

Gimpel, Henner; Röglinger, Maximilian (2015): Digital Transformation: Changes and Chances – Insights based on an Empirical Study. Hg. v. Project Group Business and Information Systems Engineer-ing (BISE) of the Fraunhofer Institute for Applied Information Technology FIT, Augsburg/Bayreuth. Available online: https://www.fim-rc.de/wp-content/uploads/Fraunhofer-Studie_Digitale-Transformation.pdf, last checked: 11.04.2019.

Glaser, Florian (2017): Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain-enabled System and Use Case Analysis. In: Proccedings of the 50th Hawaii International Conference on System Sciences, S. 1543–1552.

Le Hors, Arnaud; Ferris, Christopher; Singh, Gari (2018): Hyperleder Fabric. Architecture Explained. In cooperation with github.com. Hg. v. hyperledgerfabric.readthedocs.io. Available online: http://hyperledger-fabric.readthedocs.io/en/release-1.1/archdeep-dive.html, last checked: 11.04.2019.

Linux Foundation (2017): Hyperledger Architecture Vol. I. Introduction to Hyperledger Business Blockchain Design Philosophy and Consensus. In cooperation with ipin Bharathan, Mic Bowman, Sally Cole, Silas Davis, Nathan George, Gordon Graham, Lovesh Harchandani, Ram Jagadeesan, Tracy Kuhrt, Stanislav Liberman, Todd Little, Dan Middleton, Hart Montgomery, Binh Nguyen, Vinod Panicker, Mark Parzygnat, Vitor Quaresma, Greg Wallace. Hg. v. Linux Foundation. Available online: https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf, last checked: 11.04.2019.

Osterland, Thomas; Rose, Thomas (2018): Engineering sustainable blockchain applications. In: ER-CIM-Blockchain 2018: Blockchain Engineering: Challenges and Opportunities for Computer Science Research. Available online: https://dl.eusset.eu/handle/20.500.12015/3161, last checked: 11.04.2019.

Porru, Simone; Pinna, Andrea; Marchesi, Michele; Tonelli, Roberto (2017): Blockchain-oriented software engineering: Challenges and new directions. In: 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C), S. 169–171.

Sajana, P.; Sindhu, M.; Sethumadhavan, M. (2018): On Blockchain Applications: Hyperledger Fabric and Ethereum. In: International Journal of Pure and Applied Mathematics 18 (118), S. 2965–2970.

Schweizer, André; Schlatt, Vincent; Urbach, Nils; Gilbert, Fridgen (2017): Unchaining Social Businesses - Blockchain as the Basic Technology of a Crowdlending Platform. In: Yong Jin Kim, Ritu Agrawal und Jae Kyu Lee (Hg.): Proccedings of the 38th International Conference on Information Systems. Seoul, South Korea.

Disclaimer

This whitepaper has been prepared by the Project Group Business & Information Systems Engineering of the Fraunhofer Institute for Applied Information Technology FIT to the best of their knowledge and with due diligence.

Fraunhofer FIT, its legal representatives and/or proxies do not guarantee that the contents of this whitepaper are ascertained, entirely usable for certain purposes or otherwise free of errors. You use this whitepaper solely at your own risk.

In no event shall Fraunhofer FIT, its legal representatives and/or proxies be liable for any direct or indirect damages incurred by the use of this whitepaper.

Publishing information

Publisher:
Federal Office for Migration and Refugees
90461 Nuremberg, Germany

Editor:
Project Group Business & Information Systems Engineering of the Fraunhofer Institute for Applied Information Technology FIT

Date:
08/2019

Printed:
Federal Office for Migration and Refugees, 90461 Nuremberg, Germany

Design:
DOK SYSTEME Ingenieurgesellschaft für Kommunikationstechnik mbH

Picture credits:
Cover picture: © iStock matejmo; Figure 1: © BAMF, Landscape of Germany ©Shutterstock, Filip Bjorkman; Alle other figures: © Fraunhofer FIT; ©DOK SYSTEME Ingenieurgesellschaft für Kommunikationstechnik mbH

Recommended citation:
Fridgen, G., Guggenmos, F., Lockl, J., Rieger, A.; Urbach, N. and Wenninger, A. 2019. Development of a GDPR-compliant Blockchain Solution for the German Asylum Procedure: A pilot project in the context of the AnkER-facility in Dresden. Project Group Business & Information Systems Engineering of the Fraunhofer Institute for Applied Information Technology FIT, ed. Federal Office for Migration and Refugees (Nuremberg)

Available to order:
Publication office of the BAMF
www.bamf.de/publikationen

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

Visit us at:
www.facebook.com/bamf.socialmedia
@BAMF_Dialog
www.bamf.de/blockchain