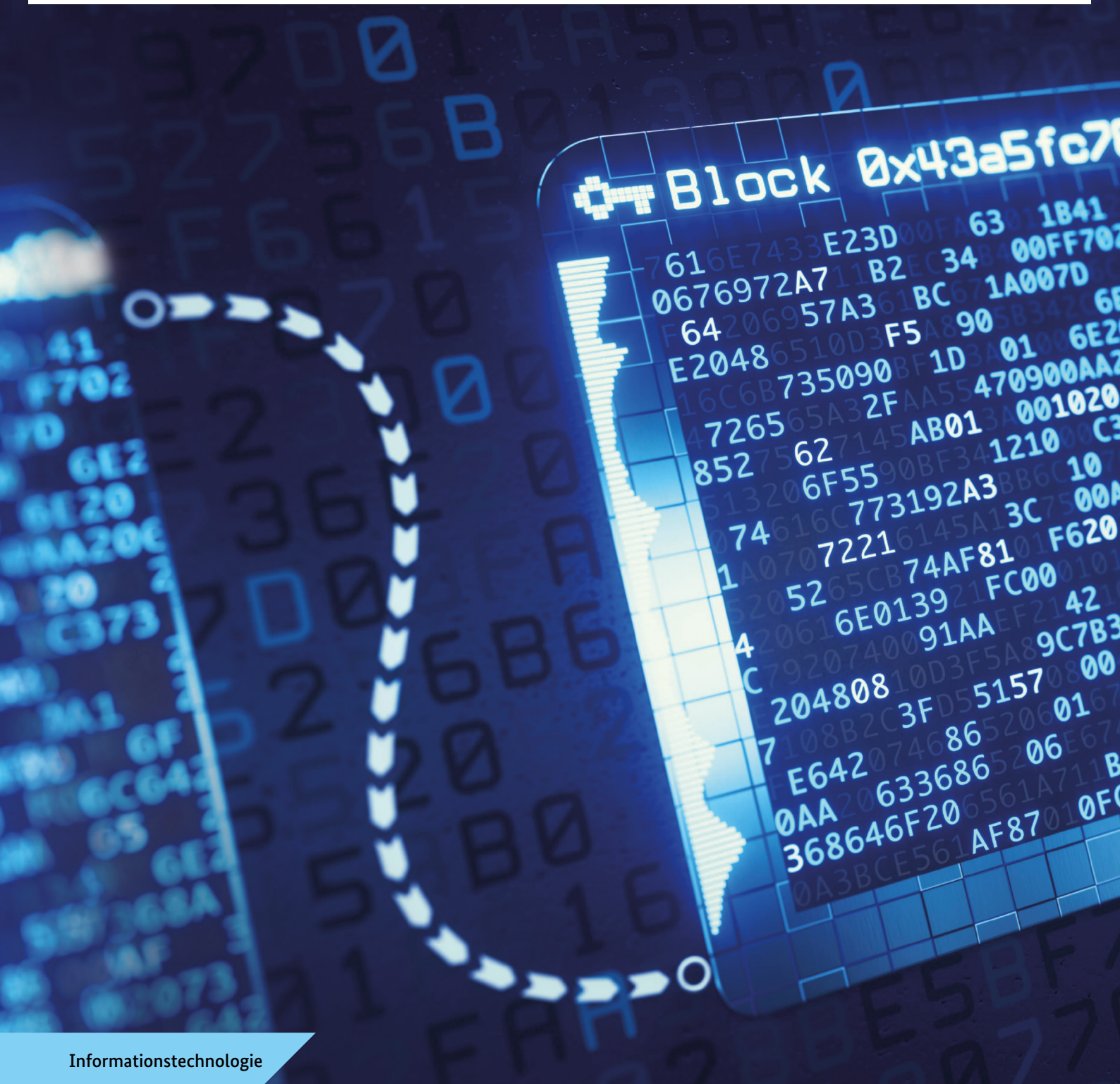


Entwicklung einer datenschutzkonformen Blockchain-Lösung im deutschen Asylprozess

Pilotierung im Kontext der AnKER-Einrichtung Dresden



Entwicklung einer datenschutzkonformen Blockchain-Lösung im deutschen Asylprozess

Pilotierung im Kontext der AnkER-Einrichtung Dresden

Whitepaper der Projektgruppe

Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT

Kurzfassung

Digitale Transformation bedeutet, bestehende Abläufe und Prozesse neu zu denken, neue Arbeitsweisen zu etablieren und innovative Denkweisen zu fördern. Digitale Transformation kann zudem helfen, die fragmentierte Systemlandschaft der deutschen Verwaltung zu verbessern, welche die Kommunen, Landes- und Bundesbehörden zunehmend vor Herausforderungen stellt. Eine der digitalen Fokus-Technologien in diesem Kontext ist die Distributed-Ledger-Technologie und ihre prominenteste Vertreterin, die Blockchain-Technologie.

Der Einsatz von Distributed-Ledger-Technologie verkörpert eine bewusste Abkehr von Konsolidierungsansätzen hin zu einer Abbildung föderaler Strukturen und Prinzipien auch in der digitalen Infrastruktur der deutschen Verwaltung. Die Blockchain ist insbesondere bei der Prozessoptimierung in föderalen Strukturen hilfreich, wenn eine intensive Kommunikation und enge Zusammenarbeit trotz starker organisatorischer Heterogenität erforderlich sind.

In diese Kategorie fällt auch der deutsche Asylprozess. An diesem ist eine Vielzahl unterschiedlicher Behörden auf Ebene des Bundes und der Länder beteiligt. Insbesondere auf Landesebene existieren zudem unterschiedliche Prozessvarianten und Abläufe, was eine zentrale Steuerung durch ein einzelnes Workflow-Management-System faktisch unmöglich macht. Vielmehr erfordert der deutsche Asylprozess einen koordinativen Ansatz und eine verteilte IT-Lösung, welche Prozess-Updates sicher und rasch an alle beteiligten Behörden

verteilt, damit diese bei Bedarf und selbstständig koordinative Maßnahmen einleiten können.

Im Rahmen eines Proof-of-Concepts hat das Bundesamt für Migration und Flüchtlinge bereits bestätigen können, dass die Blockchain-Technologie eine sehr vielversprechende Basis für eine solche IT-Lösung sein kann. Insbesondere ihre Eigenschaft, einen gemeinsamen und persistenten Informationsstand schnell und sicher über Behördengrenzen hinweg herstellen zu können, bietet großes Potential. Die Verminderung von Vertrauensvorbehalten spielt hingegen im Asylprozess zwischen Behörden eine untergeordnete Rolle.

Nun soll die Technologie ihre Eignung auch im beschränkten Wirkbetrieb zeigen. Hierzu wird aktuell gemeinsam mit der Landesdirektion Sachsen eine Blockchain-Lösung für den Kontext der AnkER-Einrichtung Dresden entwickelt.

Das Bundesamt erwartet sich durch den Einsatz der Blockchain-Lösung einen zeitnahen und medienbruchfreien Informationsaustausch in den Teilprozessen „Registrierung, Aktenanlage und Anhörung“, „Zuweisung“, sowie „Entscheidung und Vollzug“. Durch einen derartigen Informationsaustausch würden Verfahrensdauern und Ressourcenaufwände deutlich minimiert. Zudem könnten Sicherheitsaspekte effizienter berücksichtigt werden. Weiterhin wäre einerseits eine frühzeitige Einleitung der Dokumentenbeschaffung und Organisation der Rückführung möglich. Andererseits könnten Integrationsprozesse bei positiver Entscheidung durch

eine frühzeitige Zuweisung in die Kommunen zeitnah in Gang gesetzt werden.

Das Pilotprojekt hat die Konzeptionsphase bereits weitestgehend erfolgreich abgeschlossen. In dieser Phase wurde insbesondere eine, nach aktueller Einschätzung des Bundesamtes, datenschutzkonforme Systemarchitektur implementiert, sowie ein Berichtigungs- und Löschkonzept entwickelt, um den Vorgaben und Betroffenenrechten der Datenschutz-Grundverordnung gerecht zu werden.

Zudem wurde ein Governance-Konzept entworfen, welches die Verteilung der Entscheidungskompetenzen und Verantwortlichkeiten auf datenschutzrechtlicher, technischer und organisatorischer Ebene regelt. Wesentliche Skalierbarkeitsfragen wurden in einem Skalierbarkeitskonzept adressiert.

Damit das Gesamtvorhaben seiner Rolle als Leuchtturmprojekt gerecht wird, hat das Bundesamt im Rahmen der Konzeptionierungsphase zudem mehrere grundlegende Design-Prinzipien für die Entwicklung von Blockchain-Lösungen für die öffentliche Verwaltung erarbeitet.

Sollten auch die Entwicklungs- und Evaluationsphase positiv verlaufen, sind verschiedene Ausweitungsszenarien denkbar. So könnten im ersten Schritt weitere Teilprozesse in der AnkER-Einrichtung Dresden abgebildet oder weitere Behörden im Asylprozess hinzugenommen werden. Perspektivisch ist aber auch eine EU-weite Lösung denkbar. In diesem Sinne wäre Blockchain der „digitale Enabler“

des europäischen Föderalismus im Asylkontext und könnte gar ein weiterer Schritt hin zu einem gemeinsamen Europa sein.

Inhalt

1. Motivation	10
2. Grundlage	12
2.1 Ablauf des Asylprozesses in der AnkER-Einrichtung Dresden	12
2.2 Blockchain	14
3. Pilotierung einer Blockchain-Lösung im Kontext der AnkER-Einrichtung Dresden	17
3.1 Ziele der Pilotierung	17
3.2 Anwendungsfälle	18
3.3 Herausforderung des Datenschutzes	20
4. Essentielle Konzepte für den Realbetrieb	22
4.1 Systemarchitektur	22
4.2 Löschung und Berichtigung	25
4.3 Governance	29
4.4 Skalierbarkeit	30
5. Design-Prinzipien für Blockchain-Lösungen in der öffentlichen Verwaltung	32
6. Ausblick	35
7. Literaturverzeichnis	38

Abbildungsverzeichnis

Abbildung 1: Modell-Verfahren AnKER-Einrichtungen	13
Abbildung 2: Transaktionsablauf bei Hyperledger Fabric	15
Abbildung 3: Teilprozess „Registrierung, Aktenanlage und Anhörung“	18
Abbildung 4: Teilprozess „Zuweisung“, Fallkonstellation „Gute Bleibeperspektive“	19
Abbildung 5: Teilprozess „Zuweisung“, Fallkonstellation „Dublin-Verfahren“	20
Abbildung 6: Teilprozess „Entscheidung und Vollzug“	21
Abbildung 7: Schematische Darstellung der Systemarchitektur	23
Abbildung 8: Löschung von Daten aus der Blockchain-Lösung	26
Abbildung 9: Berichtigung von Daten in der Blockchain-Lösung	28

1. Motivation

Digitale Transformation bedeutet, bestehende Abläufe und Prozesse neu zu denken, neue Arbeitsweisen zu etablieren und innovative Denkweisen zu fördern (Gimpel und Röglinger 2015). Auch der deutsche Asylprozess kann von diesen Ansätzen profitieren.

An diesem ist eine Vielzahl unterschiedlicher Behörden auf Ebene des Bundes und der Länder beteiligt. Insbesondere auf Landesebene existiert eine Vielfalt von Prozessvarianten und Vorgaben, die mittlerweile unter anderem mittels eines digitalen Dokumentenaustauschs optimiert werden. Dennoch schöpfen bisherige IT-Lösungen die Unterstützungspotentiale noch nicht vollständig aus – nicht zuletzt aufgrund fehlender wechselseitiger Anbindungen.

Eine der digitalen Technologien, welche diese Fragmentierung reduzieren könnte, ist Blockchain (Christidis und Devetsikiotis 2016; Bonneau et al. 2015). Blockchain-Lösungen ermöglichen einen sicheren, raschen und medienbruchfreien Informationsaustausch zwischen allen beteiligten Mitgliedern des Systems. So können beispielsweise der Abschluss wesentlicher Prozessfortschritte bekannt gemacht und andere Behörden befähigt werden, entsprechende Folgeschritte einzuleiten (Fridgen et al. 2018b).

Das Bundesamt für Migration und Flüchtlinge (BAMF) hat im Rahmen eines Proof-of-Concepts (PoC) bereits die Eignung der Blockchain-Technologie als digitale Infrastruktur für die Koordination föderaler Verwaltungsprozesse erprobt (Fridgen et

al. 2018a). Konkret wurde Blockchain als Technologie zur Unterstützung der behördenübergreifenden Kommunikation und Zusammenarbeit im Asylprozess eingesetzt. Hierzu wurde eine vereinfachte Version des Asylprozesses auf Blockchain-Basis abgebildet. Nach einer dreimonatigen Umsetzungsphase wurde der PoC durch Experten der Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT positiv evaluiert.

Aufbauend auf diesen Ergebnissen soll die Technologie nun auch im beschränkten Wirkbetrieb gemeinsam mit der Landesdirektion Sachsen (LDS) im Kontext der AnkER-Einrichtung Dresden erprobt werden. Die bisherigen Kommunikationswege zwischen dem Bundesamt und der LDS sind in Teilen ineffektiv, mit vielfältigen Medienbrüchen und manuellen Erfassungsvorgängen verbunden. Damit sind sie zeitaufwändig, fehleranfällig und ermöglichen insgesamt nicht unbedingt eine optimale Verfahrensabarbeitung. Durch den Einsatz von Blockchain soll ein zeitnahe und medienbruchfreier Informationsaustausch in Teilprozessen etabliert werden, so dass die Verfahrensdauer und Ressourcenaufwände deutlich minimiert und Sicherheitsaspekte effizienter berücksichtigt werden können.

Das Pilotprojekt des Bundesamtes nimmt eine wichtige Leuchtturmposition ein, da es sowohl eine konkrete Blockchain-Lösung als auch eine Reihe übertragbarer Lösungskonzepte entwickelt. Ein wesentlicher Fokus liegt dabei auf der Umsetzung datenschutzrechtlicher Details und der präzisen

Abbildung der geltenden Rechtslage. Damit das Gesamtvorhaben seiner Rolle als Leuchtturmprojekt gerecht wird, veröffentlicht das Bundesamt zu ausgewählten Zeitpunkten wichtige Erfahrungswerte (Fridgen et al. 2018a). Dieses Whitepaper spiegelt dabei die Erkenntnisse aus der Konzeptionsphase wieder.

2. Grundlage

2.1 Ablauf des Asylprozesses in der AnkER-Einrichtung Dresden

Der Asylprozess im Kontext von AnkER-Einrichtungen unterscheidet sich nicht wesentlich vom allgemeinen Asylprozess. Daher sei für eine detaillierte Beschreibung des deutschen Asylverfahrens auf das Blockchain-Whitepaper im Rahmen des PoC (Fridgen et al. 2018a) und die Broschüre des Bundesamtes für Migration und Flüchtlinge (Bundesamt für Migration und Flüchtlinge 2019) verwiesen.

AnkER-Einrichtung

„Die AnkER-Einrichtungen sind von zentraler Bedeutung, um die Asylverfahren effizienter zu gestalten, bei Menschen mit Bleibeperspektive früh mit Integrationsangeboten zu beginnen und im Falle ablehnender Entscheidungen den Prozess der Rückkehr zügig einzuleiten.“

(Dr. Hans-Eckhard Sommer, Präsident des Bundesamtes)

Das Akronym AnkER-Einrichtung steht für die Bündelung der Kompetenzen und Aufgaben von Ankunfts-, Entscheidungs- und Rückkehrreinrichtungen an einem Ort. Die Pilotierungsphase dieser Einrichtungen startete am 1. August 2018 mit der Eröffnung von sieben Einrichtungen in Bayern (Augsburg, Bamberg, Deggendorf, Manching, Regensburg, Schweinfurt und Zirndorf) sowie einer Einrichtung in Sachsen (Dresden).

Ziel in AnkER-Einrichtungen ist es, den Asylprozess durch einen räumlichen Zusammenschluss föderal zuständiger Behörden, sowohl auf Bundes-, Landes- als auch Kommunalebene, unter einem Dach effizienter zu gestalten. Durch die örtliche Nähe der Behörden und Ansprechpersonen sollen insbesondere der gegenseitige Austausch und das reibungslose Ineinandergreifen der einzelnen Prozessschritte gewährleistet werden.

Im August 2018 starteten sieben AnkER-Einrichtungen in Bayern sowie eine weitere in Sachsen. In der Pilotierungsphase werden dort bis Anfang 2020 vordefinierte Arbeitsprozesse rund um Ankunft, Aufenthalt und Unterbringung, Asylverfahrens- und Klagebearbeitung sowie Integration und Rückkehr hinsichtlich ihrer Umsetzung und ihres Nutzens getestet. Ziel der AnkER-Einrichtungen ist es, bei Menschen mit Bleibeperspektive früh mit Integrationsangeboten (z. B. Alltagsorientierung, Berufsvorbereitungen, etc.) zu beginnen und im Falle ablehnender Entscheidungen den Prozess der Rückkehr zügig einzuleiten.

Die AnkER-Einrichtungen bündeln Kompetenzen von Bund, Ländern und Kommunen. So können an einer AnkER-Einrichtung neben dem Bundesamt weitere Behörden, wie z.B. die zuständigen Ausländerbehörden, die Aufnahmeeinrichtungen der jeweiligen Länder, Verwaltungsgerichte, Bundes- und Landespolizei, Jugendämter, Gesundheitsämter, die Bundesagentur für Arbeit sowie Sozialbehörden beteiligt sein.



Abbildung 1: Modell-Verfahren Anker-Einrichtungen

Die Verantwortung für die AnkER-Einrichtungen obliegt wiederum dem jeweiligen Land. Daher können die verschiedenen Länder bei der Prozessgestaltung unterschiedliche Schwerpunkte setzen. Abbildung 1 zeigt eine schematische Darstellung der Kernprozesse der AnkER-Einrichtungen. Im Vergleich zum allgemein Asylprozess (Bundesamt für Migration und Flüchtlinge 2019) wurde der Asylprozess im Kontext der AnkER-Einrichtungen leicht angepasst beziehungsweise erweitert (Bundesamt für Migration und Flüchtlinge 2018). Die wichtigsten Änderungen betreffen die Identitätsprüfung, die Asylverfahrens- und Rückkehrberatung sowie die räumliche Einbindung von Rechtsantragsstellen. Im konventionellen Asylprozess findet eine Identitätsprüfung erst während des Asylverfahrens statt. Im Asylprozess in AnkER-Einrichtungen wurde dieser Prozessschritt nach vorne verschoben, so dass nun bereits bei der Registrierung eine umfangreiche Identitätsprüfung inklusive Verifizierung der Ausweisdokumente stattfindet. Zudem wurde die Asylverfahrensberatung des Bundesamtes als neues Element in den Gesamtprozess eingeführt. Sie wird allen Asylsuchenden vor der Antragstellung angeboten, um diese frühzeitig über den Ablauf sowie ihre Rechte und Pflichten im Asylprozess aufzuklären. Zudem können Asylsuchende, insbesondere bei denen eine ablehnende Entscheidung vorliegt, eine Beratung hinsichtlich verschiedener Möglichkeiten der Rückkehr sowie bestehender Rückkehr-Förderprogramme erhalten. Je nach örtlichen Gegebenheiten kann eine verwaltungsgerichtliche Prüfung der Asylentscheidung unter anderem über sogenannte Rechtsantragsstellen direkt in der AnkER-Einrich-

tung veranlasst werden. Damit wird der Zugang zu den Verwaltungsgerichten erleichtert.

2.2 Blockchain

Blockchain ist eine transparente, transaktionale, verteilte Datenbankstruktur, welche Daten dezentral in einem Peer-to-Peer-Netzwerk speichert (Glaser 2017). Durch einen sogenannten Konsensmechanismus bestimmt das Netzwerk gemeinsam, und nicht eine zentrale Instanz, die richtige Reihenfolge der Transaktionen in den Blöcken sowie die kryptographische und chronologische Verkettung der Blöcke (Schweizer et al. 2017). Der Konsensmechanismus und die genutzten kryptographischen Mechanismen gewährleisten Zuverlässigkeit, Gültigkeit, Sicherheit und Vertrauen im Netzwerk (Christidis und Devetsikiotis 2016; Porru et al. 2017).

Die Wahl des Konsensmechanismus ist unter anderem abhängig von der gewünschten Ausgestaltung des Blockchain-Netzwerkes entlang der zwei Dimensionen „Teilnahme“ und „Genehmigung“. In einer öffentlichen Blockchain steht die Teilnahme am Netzwerk jeder Partei offen, wohingegen in einer privaten Blockchain nur ausgewählte Parteien teilnehmen können. Hinsichtlich Genehmigung kann man zwischen genehmigungsfreien Blockchains (permissionless), in der jede teilnehmende Partei sowohl Lese- als auch Schreibrechte besitzt, und genehmigungspflichtigen Blockchains (permissioned), welche die Rechte der Teilnehmenden kontrollieren, unterscheiden (Sajana et al. 2018; Androulaki et al.

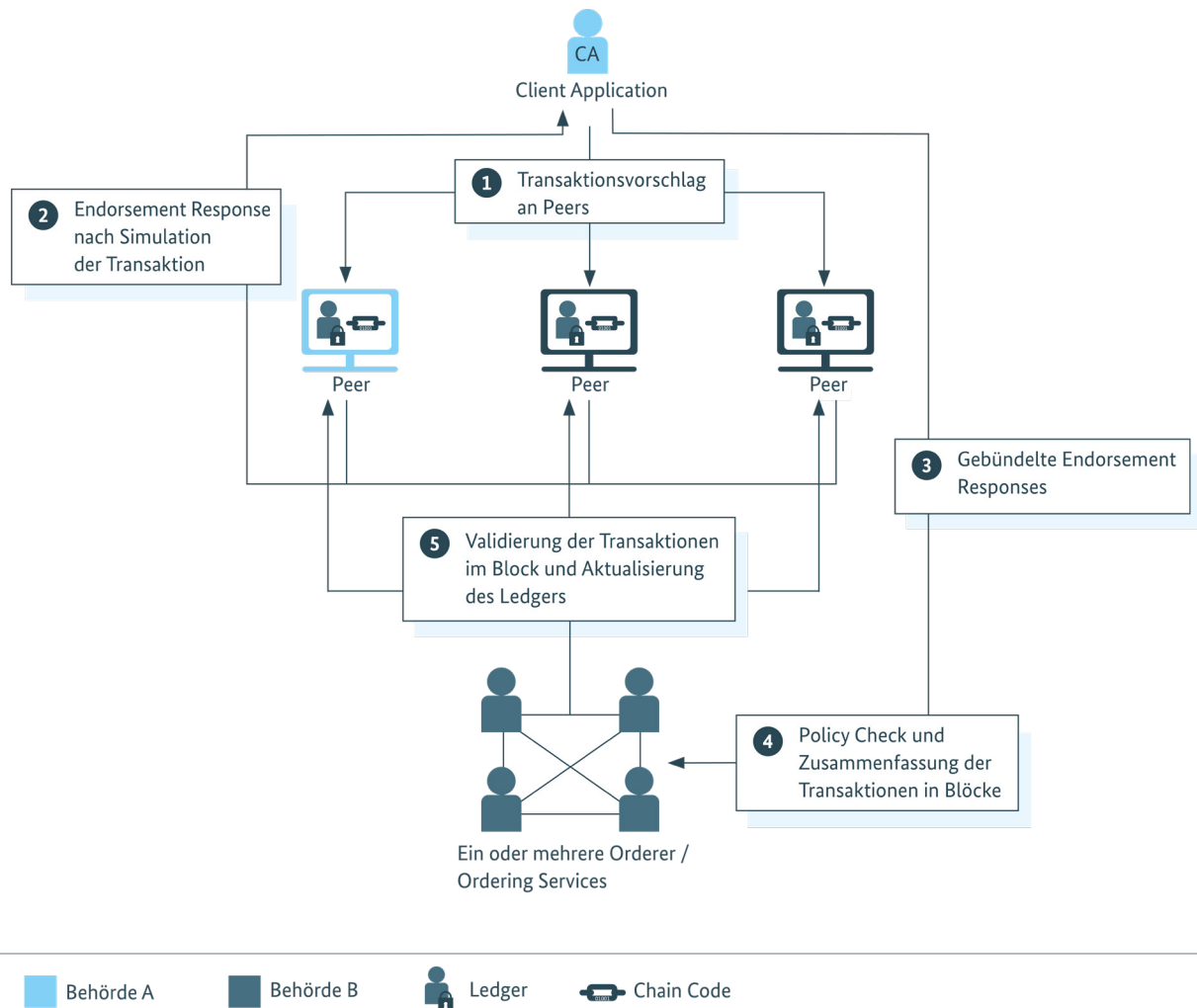


Abbildung 2: Transaktionsablauf bei Hyperledger Fabric

2018). Der eingeschränkte Zugang in privaten Blockchain-Netzwerken reduziert die Sicherheitsanforderungen an den Konsensmechanismus; so können beispielsweise Mechanismen gewählt werden, in denen die Mitglieder zufällig abwechselnd die Korrektheit der Transaktionen bestätigen. Derartige Konsensmechanismen sind mit deutlich höheren Transaktionsraten und geringeren Ressourcenverbräuchen verbunden.

Neben der Ausgestaltung des Blockchain-Netzwerkes und des Konsensmechanismus gibt es eine Vielzahl weiterer Unterscheidungsmöglichkeiten, wie beispielsweise die Art der kryptographischen Verknüpfung. Die meisten Blockchain-Technologien bieten zudem die Möglichkeit, Prozesslogiken in sogenannten Smart Contracts abzubilden und automatisch auszuführen, sobald entsprechend definierte Auslöser eintreten. Es gibt also nicht „die eine“ Blockchain.

Entsprechend hat das Bundesamt eine umfassende Bestandsanalyse bestehender Blockchain-Technologien durchgeführt. Ein besonderer Fokus lag hierbei auf Ethereum und Hyperledger Fabric. Schlussendlich fiel die Wahl auf Hyperledger Fabric, da es speziell für organisationale Anwendungsfälle entwickelt wurde.

Hyperledger Fabric ist eines der Hyperledger-Projekte, welche aktuell unter der Ägide der Linux Foundation entwickelt werden (Linux Foundation 2017). Anders als z. B. die Bitcoin-Blockchain und Ethereum setzt Hyperledger Fabric auf eine private und genehmigungspflichtige Ausgestaltung.

Konkret besitzt es einen modularen und flexiblen Aufbau, der eine leichte Anpassung einzelner Komponenten an die Anforderungen des Anwendungsfalls sowie eine gezielte Erweiterung um neue Ansätze und technologische Möglichkeiten unterstützt. Zudem bietet Hyperledger Fabric gute Skalierbarkeitseigenschaften (Linux Foundation 2017; Osterland und Rose 2018) und die Verankerung unter dem Schirm der Linux Foundation verspricht eine verlässliche und langfristige Weiterentwicklung. Außerdem lässt sich Hyperledger Fabric leicht auf verschiedenen physischen und virtuellen Infrastrukturen betreiben und es unterstützt eine Vielzahl von Programmiersprachen zur Abbildung von Smart Contracts (Sajana et al. 2018; Linux Foundation 2017; Androulaki et al. 2018).

Die genaue Funktionsweise von Hyperledger Fabric basiert auf drei verschiedenen Rollen im Netzwerk: Client, Peer und Orderer, wobei die Rolle des Peers noch in Endorser und Committer aufgegliedert werden kann (Linux Foundation 2017). Der Client erstellt im Auftrag des Endnutzenden Transaktionen und reicht diese mit der Bitte um Überprüfung bei den Endorsern ein. Die Endorser simulieren die Transaktionen und geben eine Rückmeldung bezüglich Richtigkeit sowie ein Read/Write Set an den Client zurück. Im Nachgang leitet der Client die überprüften Transaktionsvorschläge an die Orderer (auch Ordering Services genannt), welche Transaktionen, nach syntaktischer Überprüfung der Endorsement Policy, in Blöcken zusammenfassen. Die fertigen Blöcke werden daraufhin wieder zu den Peers, genauer gesagt zu den Committern geschickt. Dadurch stellt der Orderer letztendlich sicher, dass alle Peers die gleichen Transaktionen in exakt der gleichen logischen Reihenfolge erhalten. Die Committer überprüfen, ob alle vorherigen Konsensschritte inhaltlich korrekt ausgeführt wurden und keine in der Zwischenzeit durchgeführten Veränderungen der Blockchain zu einer nachträglichen Ungültigkeit der Transaktionen geführt haben, bevor sie die neuen Blöcke zur Blockchain hinzufügen (Le Hors et al. 2018). In der Blockchain werden generell alle Transaktionen aufgenommen, wobei ungültige Transaktionen gekennzeichnet werden. Abbildung 2 visualisiert den Transaktionsablauf von Hyperledger Fabric.

3. Pilotierung einer Blockchain-Lösung im Kontext der AnkER-Einrichtung Dresden

3.1 Ziele der Pilotierung

Das übergeordnete Ziel des Blockchain-Pilotprojektes liegt in der Entwicklung einer funktionsfähigen Blockchain-Lösung und seiner Erprobung im beschränkten Wirkbetrieb. Dabei sollen insbesondere Fragen der Akzeptanz, der Wirtschaftlichkeit, des Potentials und der technischen Optimierung beantwortet werden. Neben den strategischen und fachlichen Zielen sind auch die Nichtziele des Pilotprojektes klar definiert.

Strategische Ziele

1. Das Pilotprojekt soll einen wesentlichen Beitrag zum Wissensaufbau und zwischenbehördlichen Austausch zu den Einsatzmöglichkeiten der Blockchain-Technologie im Bereich der öffentlichen Verwaltung in Deutschland leisten.
2. Das Pilotprojekt soll beleuchten, ob die Blockchain-Technologie im öffentlichen Sektor als Technologie im Sinne des Koalitionsvertrages sinnvoll einsetzbar ist.
3. Das Pilotprojekt soll im Falle einer positiven Evaluierung fundierte Vorschläge zur Etablierung eines Standards für den Einsatz von Blockchain-Technologien in anderen Behörden liefern.

Fachliche Ziele

1. Die Blockchain-Lösung soll die Transparenz, die Produktivität und die Effizienz der Zusammenarbeit der LDS und des Bundesamtes in der AnkER-Einrichtung Dresden steigern. Insbesondere ihre Eigenschaft, einen gemeinsamen und persistenten Informationsstand schnell und sicher über Behördengrenzen hinweg herstellen zu können, bietet großes Potential. Die Verminderung von Vertrauensvorbehalten spielt hingegen im Asylprozess eine untergeordnete Rolle.
2. Die Blockchain-Lösung soll präventiv vor Abweichungen im Standardprozess in der AnkER-Einrichtung Dresden warnen und diese Vorkommnisse gegebenenfalls protokollieren.
3. Die Blockchain-Lösung soll die Bearbeitung der ausgewählten Prozessschritte im Asylprozess beschleunigen.
4. Die Informationsgüte bei der Entscheidung über Asylanträge und die Rechtssicherheit bei der Registrierung, Aktenlage und Anhörung sollen gesteigert werden.

Nicht-Ziele

1. Die Blockchain-Lösung soll weder die Bestandsysteme des Bundesamtes noch der Landesdirektion Sachsen ablösen.

- Die implementierte Blockchain-Lösung soll nicht zur elektronischen Leistungskontrolle verwendet werden können und keinen Zugriff auf Massendaten ermöglichen.

3.2 Anwendungsfälle

Im Rahmen des Pilotprojektes werden drei Teilprozesse „Registrierung, Aktenanlage und Anhörung“, „Zuweisung“, sowie „Entscheidung und Vollzug“ durch die Blockchain-Lösung unterstützt. Diese Teilprozesse wurden ausgewählt, da sie eine enge Zusammenarbeit und Abstimmung zwischen dem

Bundesamt und der LDS erfordern.

In allen drei Teilprozessen werden lediglich die Abläufe beim Bundesamt und der LDS betrachtet, die durch die Blockchain-Lösung unterstützt werden. Prozessschritte weiterer beteiligter Behörden (z.B. das Gesundheitsamt bei der Registrierung) sind nicht Teil der Pilotierung.

Der Teilprozess „Registrierung, Aktenanlage und Anhörung“ lässt sich fachlich tiefer in neun Vorgänge untergliedern. Abbildung 3 zeigt eine schematische Darstellung der in diesem Teilprozess vorhandenen Vorgänge sowie die einzelnen zu evaluierenden Prozessschritte auf Seiten des Bundesamtes sowie der LDS.



Abbildung 3: Teilprozess „Registrierung, Aktenanlage und Anhörung“

Der Teilprozess „Zuweisung“ lässt sich in die Fallkonstellation „Gute Bleibeperspektive“ und „Dublin-Verfahren“ unterscheiden. In Abbildung 4 ist die Fallkonstellation „Gute Bleibeperspektive“ schematisch abgebildet. Diese Variante lässt sich fachlich tiefer in sechs Vorgänge untergliedern, wenn eine positive Entscheidung, also eine positive Bleibeperspektive, vorliegt.

In Abbildung 5 hingegen ist die zweite Variante der Zuweisung, wenn ein Dublin-Verfahren in Betracht kommt, abgebildet. Im Dublin-Verfahren wird festgestellt, welcher EU-Mitgliedstaat für die Prüfung eines Asylantrags zuständig ist. Ergibt die Prüfung

durch das Dublin-Zentrum, dass ein anderer Mitgliedstaat für die Bearbeitung des Asylantrages zuständig sein könnte, wird ein sogenanntes Übernahmeersuchen an den betreffenden Mitgliedstaat gerichtet. Stimmt der Mitgliedstaat dem Übernahmeersuchen zu, stellt das Bundesamt die Unzulässigkeit des Asylantrages fest und fordert die Antragsstellenden zur Ausreise in diesen Mitgliedstaat auf. Für den Fall, dass dieser Ausreiseaufforderung nicht nachgekommen wird, ordnet das Bundesamt die Abschiebung in diesen Mitgliedstaat an. Wird hingegen kein Dublin-Verfahren durchgeführt oder dieses abgebrochen, dann kann es zur landesinternen Verteilung, wie im Teilprozess „Zuweisung“, kommen.

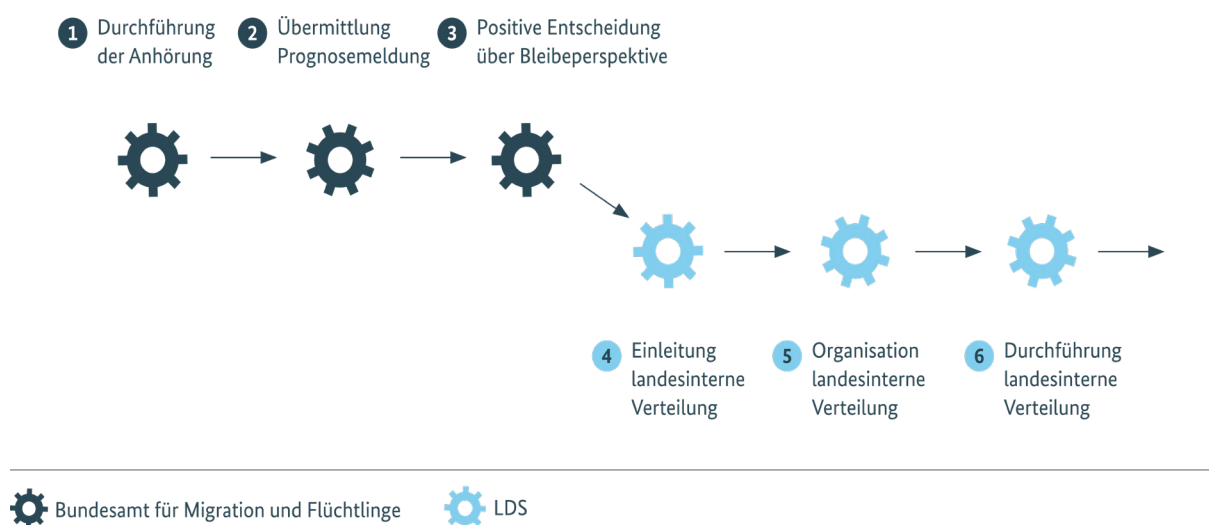


Abbildung 4: Teilprozess „Zuweisung“, Fallkonstellation „Gute Bleibeperspektive“

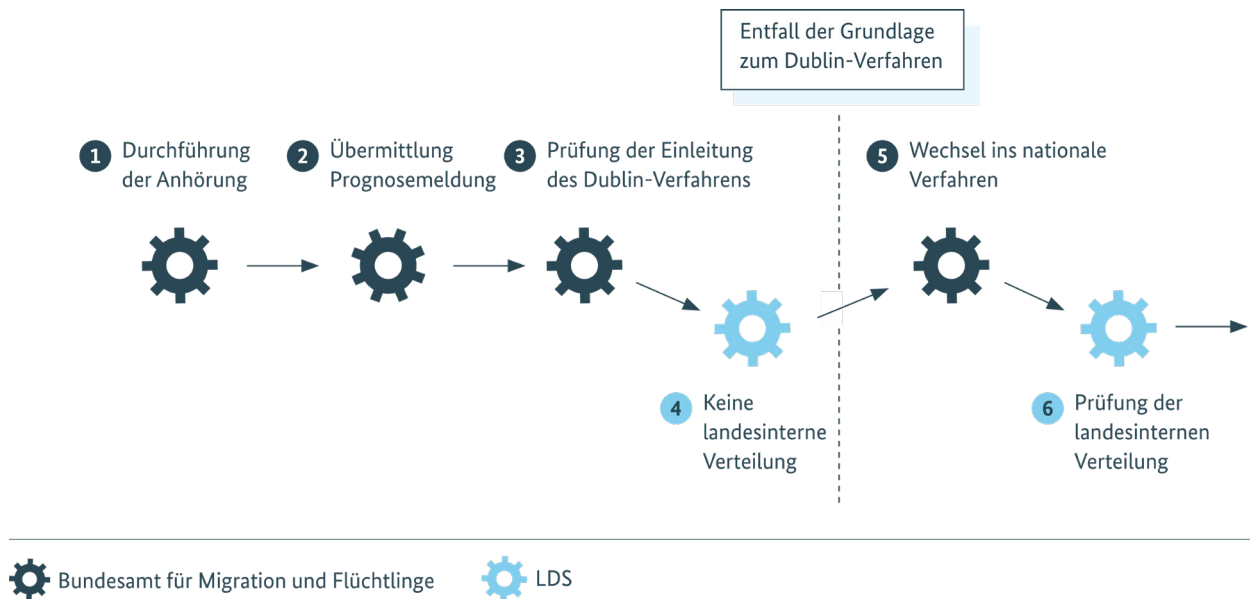


Abbildung 5: Teilprozess „Zuweisung“, Fallkonstellation „Dublin-Verfahren“

Der Teilprozess „Entscheidung und Vollzug“, dargestellt in Abbildung 6, lässt sich abhängig von der Entscheidung bezüglich des Asylgesuchs in fünf bis sechs fachlich tiefere Vorgänge untergliedern. Dabei sind aber nicht alle Vorgänge verpflichtend.

3.3 Herausforderung des Datenschutzes

Am 25. Mai 2018 ist die Datenschutz-Grundverordnung (DSGVO) in Kraft getreten. Die DSGVO regelt einheitlich den Schutz und die Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen (Daten verarbeitende Stelle) in der Europäischen Union. Neben allgemeinen Regeln

und Vorschriften für die Speicherung und automatische Verarbeitung personenbezogener Daten stärkt die DSGVO auch die Rechte der betroffenen Person (Kapitel 3, Artikel 12–23 DSGVO). Zu diesen Rechten gehört unter anderem das Recht auf Berichtigung (Artikel 16 DSGVO) sowie das Recht auf Löschung („Recht auf Vergessenwerden“) (Artikel 17 DSGVO). Das Recht auf Berichtigung regelt, dass die verantwortliche Stelle zur Datenverarbeitung unrichtige, nicht aktuelle oder unvollständige personenbezogene Daten unverzüglich korrigieren muss. Gemäß dem Recht auf Löschung können Betroffene die Löschung ihrer personenbezogenen Daten verlangen, wenn die Aufbewahrung der Daten für den Zweck, zu dem sie ursprünglich erhoben wurden, nicht mehr erforderlich ist, die Daten unrechtmäßig verarbeitet wurden oder die betroffene Person ihre Einwilligung für eine

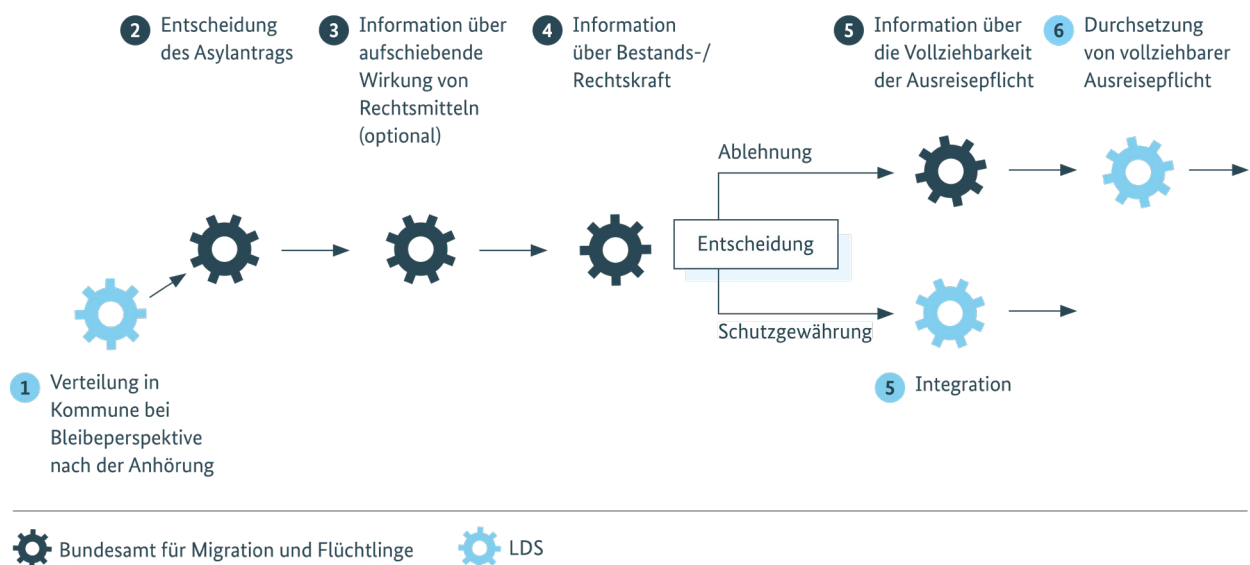


Abbildung 6: Teilprozess „Entscheidung und Vollzug“

weitere Speicherung widerrufen hat. Eine besondere Form des Lösungsanspruchs ist das „Recht auf Vergessenwerden“. Dieses Recht bezieht sich auf Daten, die veröffentlicht wurden, und zielt insbesondere auf Veröffentlichungen im Internet ab.

Die Einhaltung der Individualrechte der DSGVO zeigt allerdings den technischen Möglichkeiten von Blockchain gewisse Anwendungsgrenzen auf. Zum einen gelten Blockchain-Lösungen durch die „Verhasung“ der Blöcke als unveränderbar und insbesondere nicht löschar, weswegen im Hinblick auf das Recht auf Berichtigung und das Recht auf Löschung einige Herausforderungen bestehen. Zudem schreibt die DSGVO vor, dass klar definiert sein muss, wer die Verantwortung für die Sicherstellung der Einhaltung der DSGVO übernimmt. Dies ist insbesondere dann

wichtig, wenn mehrere Parteien gemeinsam die Verarbeitung personenbezogener Daten kontrollieren, wie es bei dezentralen Systemen und insbesondere in Blockchain-Netzwerken grundsätzlich der Fall ist. Hierzu müssen zwischen den Parteien Vereinbarungen zur transparenten Verteilung der entsprechenden Verantwortungsbereiche und Pflichten getroffen werden.

Die DSGVO erstreckt sich in ihrem Anwendungsbereich auch auf die Verwaltung. Daher wurde für das Pilotprojekt eine, nach aktueller Ansicht des Bundesamtes, datenschutzkonforme Architektur sowie ein Berichtigungs- und Löschkonzept entwickelt, welche die Einhaltung der Betroffenenrechte in Kapitel 16 und 17 der DSGVO sicherstellen. Näheres hierzu findet sich in Kapitel 4 dieses Whitepapers.

4. Essentielle Konzepte für den Realbetrieb

4.1 Systemarchitektur

Die Architektur der Blockchain-Lösung gliedert sich in drei Ebenen (siehe Abbildung 7). Diese umfassen auf der untersten Ebene die aktuellen Bestandsysteme der jeweiligen Behörden. Darüber befindet sich die Integrationsebene. Diese Ebene besteht zum einen aus einer Dashboard-Schicht, in der je nach Rolle und Rechten der Behörde Inhalte aus der Bestandssystem-Schicht sowie der Blockchain-Ebene dargestellt werden können. Zudem umfasst die Integrationsebene die sogenannte Privacy-Service-Schicht, welche ein datenschutzfreundliches Mapping der eindeutigen, pseudonymisierten Zuordnungsmerkmale auf der Blockchain und der fachlichen Merkmale in den Bestandssystemen ermöglicht. Die Integration der Dashboard- und Privacy-Service-Schicht kann sich von Behörde zu Behörde unterscheiden, wobei bei der Ausgestaltung behördenübergreifende Rahmenbedingungen befolgt werden müssen.

Einheitlich ausgestaltet im Hinblick auf Integration und technische Ausgestaltung ist nur die dritte Ebene, auf der Prozessupdates über die Blockchain geteilt werden können. Die Blockchain verbindet die verschiedenen Bestandsysteme zu einem Netzwerk, in dem Informationen gesichert untereinander geteilt werden können. Die Blockchain-Ebene dient also als „technologische und informationstechnische Klammer“ über die verschiedenen Bestandsysteme.

Die Schnittstellen zwischen der Privacy-Service-Schicht und der Blockchain-Ebene erfolgt über standardisierte und abgesicherte Schnittstellen. Dies ermöglicht eine vergleichsweise einfache Skalierung, da die Dashboard- und Privacy-Service-Schicht gemäß den Anforderungen einer neu hinzuzunehmenden Behörde gestaltet und per Standardschnittstelle an die Blockchain angeschlossen werden können.

Blockchain-Ebene

Die Blockchain-Ebene umfasst eine private, permissioned Blockchain auf Basis von Hyperledger Fabric. Aus Gründen der Einfachheit sieht die aktuelle Planung vor, dass die Blockchain-Knoten für die Pilotierung in einer mandantenfähigen Cloud-Umgebung des Bundesamtes gehostet und betrieben werden. Die Konsensfindung erfolgt auf Basis eines noch zu bestimmenden gängigen Konsens-Algorithmus. Der Konsensus-Algorithmus kann jedoch nachträglich durch den modularen Aufbau der gewählten Hyperledger Implementierung ausgetauscht werden.

Um die Anforderungen der DSGVO, insbesondere das Recht auf Löschung, umzusetzen, werden auf der Blockchain keine personenbezogenen Daten gespeichert. Auf der Blockchain werden nach aktueller Planung lediglich ein eindeutiges, pseudonymisiertes Zuordnungsmerkmal (Blockchain-ID) eines Asylanspruchs, der aktuelle Prozessstatus, ein Zeitstempel sowie das Kürzel der durchführenden Behörde gespeichert.

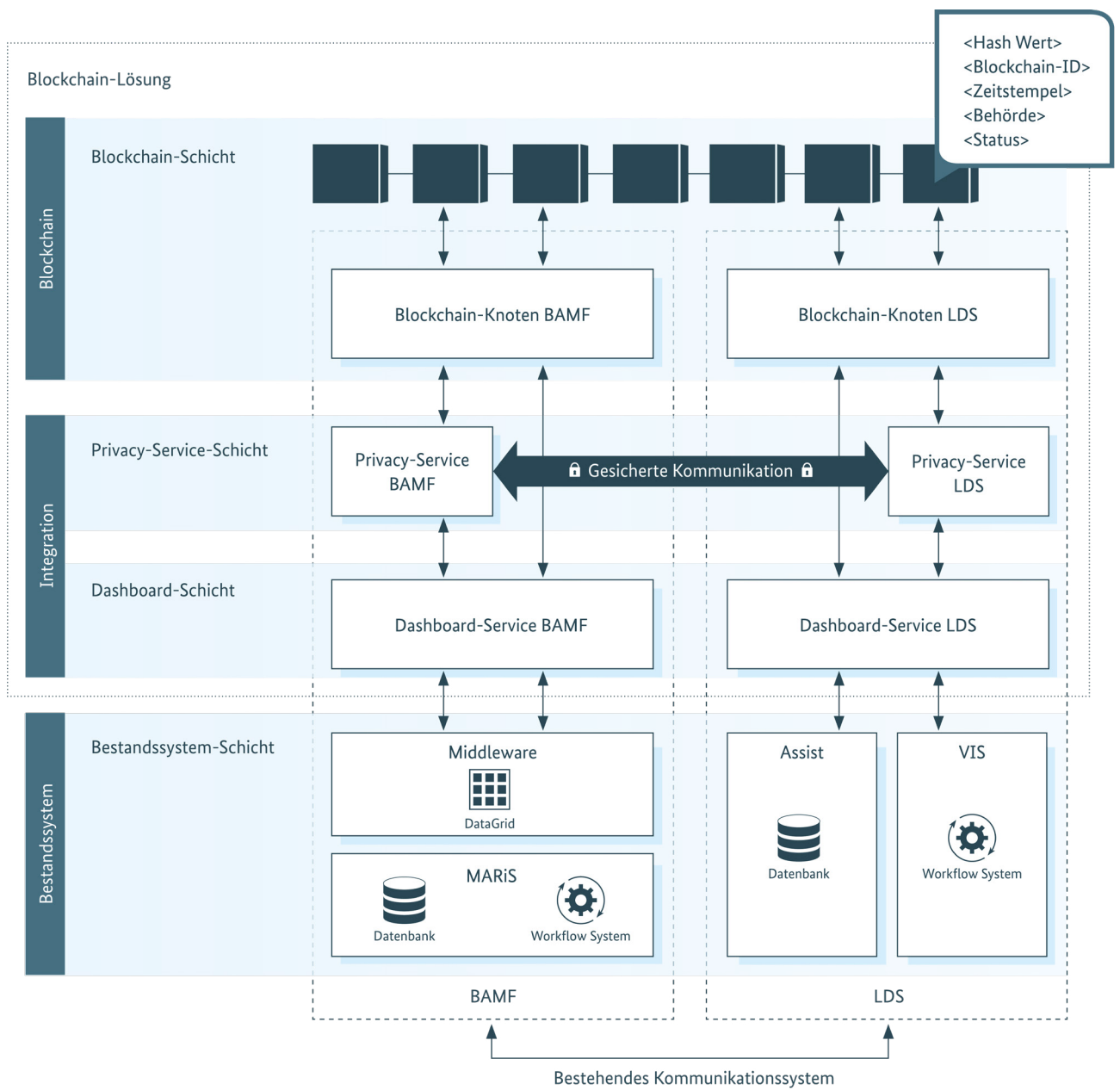


Abbildung 7: Schematische Darstellung der Systemarchitektur

Integrationsebene: Privacy-Service-Schicht

Die Hauptfunktion der Privacy-Services besteht im Wesentlichen in der datenschutzfreundlichen, d.h. lösch- und änderbaren Zuordnung der Blockchain-IDs zu den von den jeweiligen Behörden genutzten IDs (bspw. in Form von Aktenzeichen). Ohne diese Zuordnung besitzen die Status-Updates auf der Blockchain keinen verwertbaren Informationsgehalt.

Konkret ist auf der Blockchain-Ebene zwar erkennbar, welche Transaktionen bzw. Events zu einer Blockchain-ID gehören. Den jeweiligen Behörden sowie sonstigen Dritten ist es jedoch nicht möglich, ohne die Zuordnung in den Privacy-Services einen Bezug zu einem konkreten Asylverfahren und darüber hinaus zu einer konkreten antragstellenden Person herzustellen.

DataGrid

Das DataGrid entspricht einem abgesicherten Auskunftsservice. Es ermöglicht eine Entkopplung von den diversen Back-End-Systemen des Bundesamtes und bietet eine auf die Anforderungen des Nutzers zugeschnittene Haltung und Bereitstellung von Daten aus den Back-End-Systemen des Bundesamtes.

Etwas technischer gesprochen sind die Privacy-Services als hochsichere Mapping-Services konzipiert, die rollenbasierte Zugriffsverfahren für unterschiedliche Personengruppen unterstützen, die Zuordnung zwischen den fachlichen Merkmalen und den Blockchain-IDs erstellen, ändern und löschen können.

Die Privacy-Services bieten zudem die Möglichkeit, Zuordnungs-Informationen Ende-zu-Ende-verschlüsselt zwischen den Behörden über einen bestehenden Kanal off-chain auszutauschen. Dieser Austausch ist insbesondere dann wichtig, wenn die Zuständigkeit für ein Asylverfahren das erste Mal auf eine andere Behörde übergeht, um zu verhindern, dass ein Antrag mehrfach auf der Blockchain mit unterschiedlichen Blockchain-IDs erfasst wird.

Integrationsebene: Dashboard-Schicht

Zur Visualisierung des aktuellen Status von Asylgesuchen und -anträgen wurde ein Dashboard-basiertes System entwickelt, das über einen Webbrowser genutzt werden kann. Je nach Rolle und Rechte des Nutzers werden hier Inhalte dargestellt, die bei der Erfüllung der jeweiligen Aufgabe relevant sind. Diese Schicht ist über standardisierte und abgesicherte Schnittstellen an die Privacy-Service-Schicht und an die Bestandssysteme gekoppelt. Über diese Schnittstellen können über das Mapping einerseits der Status aus der Blockchain gelesen und andererseits weiterführende Daten gemäß den Berechtigungen direkt aus dem Bestandssystem geladen werden.

Bestandssystem-Ebene

Jede Behörde verwaltet aufgrund der föderalen Gesetzeslage auch weiterhin ihre Bestandssysteme selbstständig. Beim Bundesamt besteht das Bestandssystem aus Middleware Services sowie dem zentralen Workflow- und Dokumentenmanagementsystem MARiS, welches neben der Datenhaltung auch Workflow Management Funktionalitäten anbietet. Die Anbindung der Dashboard-Schicht an die Bestandssysteme des Bundesamtes erfolgt über sogenannte Middleware Services des Bundesamtes. Diese Middleware Services umfassen unter anderem das sogenannte DataGrid.

Das Bestandssystem der LDS besteht aus der Fachanwendung ASSIST inklusive diverser Datenbanken sowie dem Vorgangsverarbeitungssystem VIS.

In diesen Bestandssystemen werden auch in Zukunft alle personenbezogenen und sensiblen Daten dezentral gespeichert. Push-basierte Übermittlungen dieser Daten können reduziert werden, weil stattdessen andere Behörden diese im Falle eines berechtigten Interesses pull-basiert anfragen können. Für jede dieser Anfragen ist wiederum eine (automatisierte) Identitäts- und Berechtigungsprüfung notwendig.

Bewertung der Architektur

Durch den Verbleib der sensiblen Daten in den Bestandssystemen wird einerseits der föderalen

Struktur des Asylprozesses Rechnung getragen und ein wesentlicher Beitrag in Richtung konsequenter Umsetzung des Once-Only-Prinzips geleistet, da personenbezogene Daten nicht zusätzlich bei verschiedenen Behörden redundant gespeichert werden müssen. Andererseits können mit der Architektur die Rechte auf Berichtigung und Löschung (Artikel 16 und 17 DSGVO) gewährleistet werden. Dies wird explizit im nachfolgenden Kapitel erläutert.

Der besondere Mehrwert der Systemarchitektur besteht also darin, dass über die Blockchain operative Prozessdaten gemäß geltenden Rechtsgrundlagen (z.B. DSGVO) zwischen verschiedenen Behörden geteilt werden können, ohne dabei an Datenhoheit einzubüßen oder personenbezogene Daten direkt auf der Blockchain zu speichern.

4.2 Löschung und Berichtigung

Das Recht auf Löschung (Artikel 17 DSGVO) schreibt vor, dass personenbezogene Daten zu löschen sind, falls der Zweck ihrer Erhebung nicht mehr gegeben ist. Im Kontext des Asylverfahrens ist dies zum Beispiel dann der Fall, wenn das Asylverfahren abgeschlossen ist. Zudem schreibt das Asylgesetz vor, dass die Daten abgeschlossener Verfahren spätestens nach zehn Jahren zu löschen sind (§7 Abs. 3 AsylG).

Die Löschung von Daten betrifft alle drei Ebenen der vom Bundesamt entwickelten Blockchain-Lösung. Eine schematische Darstellung eines Löschvorgangs ist in Abbildung 8 dargestellt.

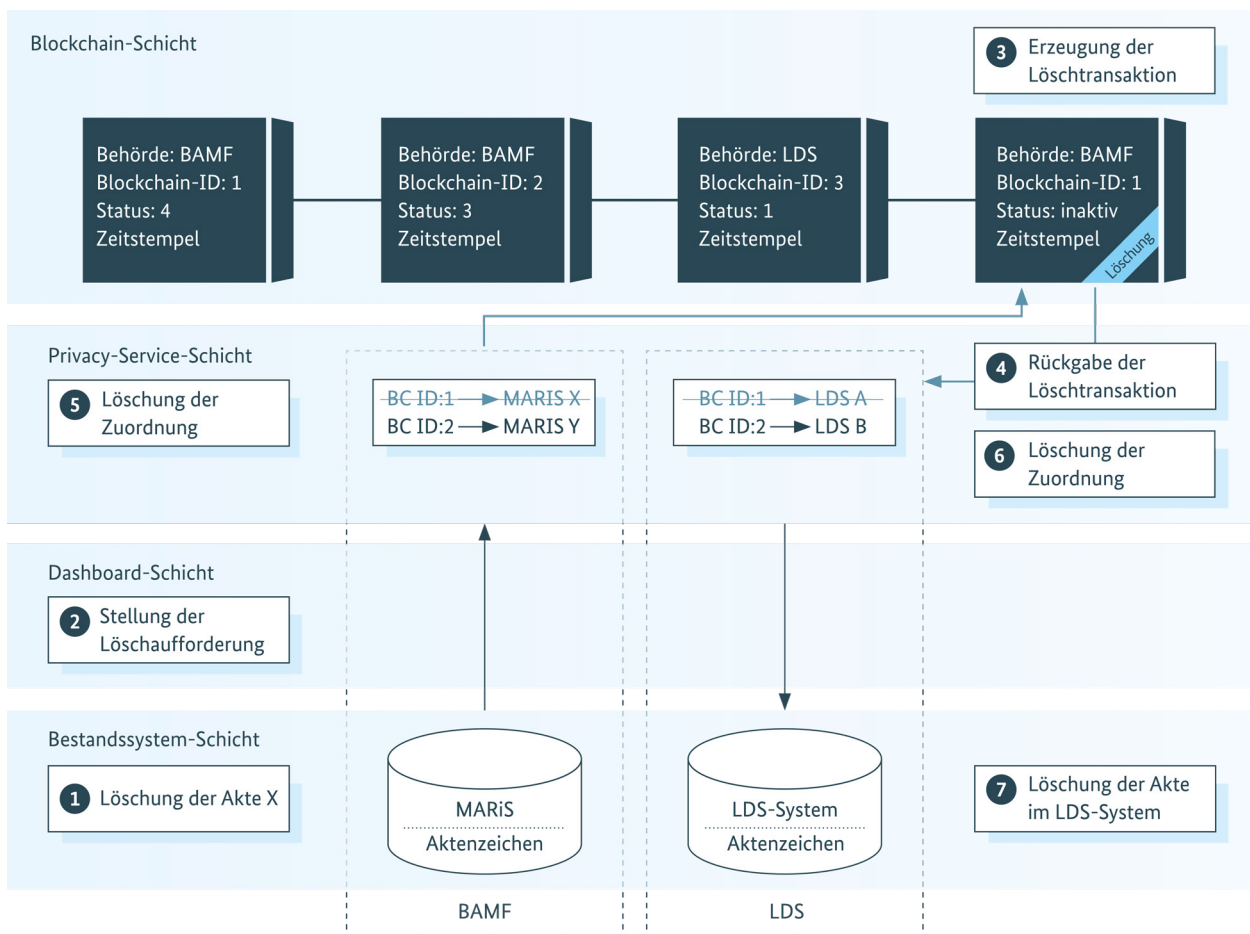


Abbildung 8: Löschung von Daten aus der Blockchain-Lösung

Zunächst werden die betroffenen Daten im eigenen Bestandssystem regulär gelöscht (Schritt 1). Anschließend wird eine Benachrichtigung über den erfolgten Löschvorgang an den behördenspezifischen Privacy-Service gesendet (Schritt 2), welcher wiederum eine sogenannte „Löschtransaktion“ auf

der Blockchain speichert (Schritt 3). Diese Löschtransaktion macht kenntlich, dass die zur jeweiligen Blockchain-ID gehörigen Prozessinformationen in dem Bestandssystem der schreibenden Behörde gelöscht wurden und die Blockchain-ID nicht mehr verwendet werden soll. Über die Blockchain

werden die anderen am Blockchain-Netzwerk teilnehmenden Behörden über die Löschung informiert (Schritt 4). Zuletzt löscht die schreibende Behörde die Zuordnung in ihrem Privacy-Service (Schritt 5) und es werden automatisch auch alle entsprechenden Zuordnungen in den Privacy-Services der anderen Behörden (in Abbildung 8 der LDS) gelöscht (Schritt 6).

Das Löschen entsprechender Daten in den Bestandssystemen anderer Behörden (Schritt 7) obliegt weiterhin ausschließlich der Verantwortung der jeweiligen Behörden. Es wird nicht über die Blockchain überwacht. Es wäre jedoch denkbar, dass alle anderen Behörden, welche auf die Löschransaktion mit der Löschung der entsprechenden Daten in ihrem Bestandssystem reagiert haben, dies ebenfalls mit einer Transaktion auf der Blockchain dokumentieren. Gleichzeitig soll durch die Blockchain-Lösung keine Behörde verpflichtet werden, Daten aus dem eigenen Bestandssystem zu löschen.

Unter der Annahme, dass im Falle einer gesetzlichen Löschpflicht alle Behörden dieser auch nachkommen und die entsprechenden Daten aus ihren Systemen entfernen, verbleiben ausschließlich die auf der Blockchain gespeicherten Statusmeldungen. Da allerdings auch die Zuordnung in den Privacy-Services gelöscht wurde, kann die jeweilige Behörde die Blockchain-ID keinem Antrag mehr eindeutig zuordnen. Ein Rückschluss auf den jeweiligen Antrag und die damit verbundene natürliche Person ist durch den verwendeten Algorithmus nicht mehr beziehungsweise nur noch mit unverhältnismäßig großem Aufwand möglich.

Neben dem Löschen stellt auch das Korrigieren falscher Angaben auf der Blockchain (Artikel 17 DSGVO) eine wichtige Komponente dar in Bezug auf die Einhaltung des Datenschutzes. Auch im Rahmen des Asylprozesses in AnKER-Einrichtungen kann es aus verschiedenen Gründen notwendig sein, auf der Blockchain gespeicherte Informationen zu berichtigen. Dies ist zum Beispiel dann der Fall, wenn durch Mitarbeitende versehentlich falsche Daten eingegeben und ein falscher Status in die Blockchain geschrieben wurde bzw. Statusmeldungen aufgrund externer Einflüsse widerrufen werden müssen.

Im Rahmen eines Korrekturvorganges wird die Korrektur wiederum zuerst im Bestandssystem vorgenommen (Schritt 1). Diese Korrektur der Daten wird danach an den Privacy-Service gemeldet (Schritt 2). Dieser erzeugt nun eine neue, sogenannte Korrekturtransaktion auf der Blockchain (Schritt 3). Diese Korrekturtransaktion macht den zu ändernden Status kenntlich und legt den nun mehr geltenden Status fest. Über die Blockchain werden die anderen am Blockchain-Netzwerk teilnehmenden Behörden über die Korrektur informiert, und diese können die Korrektur nun verarbeiten (Schritt 4). So können zum Beispiel bereits gestartete Folgeprozesse gestoppt und gegebenenfalls rückabgewickelt werden (Schritt 5). Damit können unrechtmäßige Abschiebungen verhindert werden, für die aufgrund kurzfristig eingelegter Rechtsmittel keine rechtliche Grundlage mehr besteht. Eine schematische Darstellung eines Korrekturvorganges ist in Abbildung 9 dargestellt.

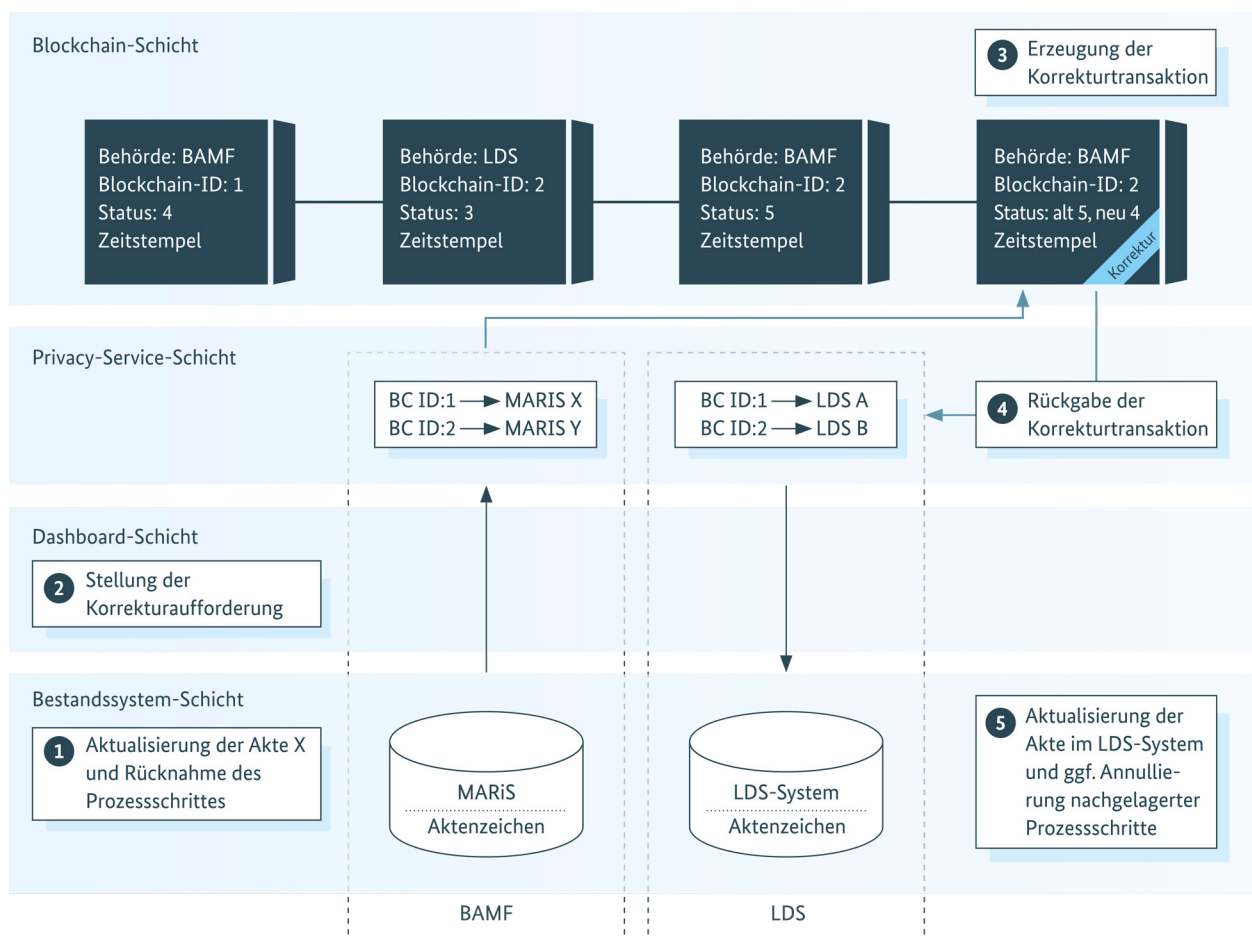


Abbildung 9: Berichtigung von Daten in der Blockchain-Lösung

4.3 Governance

Der Einsatz einer Blockchain-Lösung erfordert Koordinierung auf vielerlei Ebenen. Dies beginnt bei der Definition fachlicher Anforderungen und reicht bis zur Aufgabenverteilung im operativen Betrieb. Um die Komplexität der erforderlichen Koordinierungsprozesse zu minimieren, bedarf es einer effektiven Verteilung der Entscheidungskompetenzen und Verantwortlichkeiten, sprich einer effektiven Governance. Konkret ist eine solche Verteilung sowohl auf datenschutzrechtlicher, technischer und organisatorischer Ebene wichtig.

Datenschutzrechtliche Governance

Der Aufbau einer Blockchain-Lösung birgt eine Reihe datenschutzrechtlicher Herausforderungen. Insbesondere gilt es, eine transparente Verteilung der Verantwortlichkeiten für die Einhaltung der Vorgaben der DSGVO zu schaffen.

Technische Governance

Auch auf der technischen Ebene müssen effektive Governance-Strukturen geschaffen und Techniken eingesetzt werden, um eine effektive Entwicklung und einen reibungslosen Betrieb einer Blockchain-Lösung zu gewährleisten.

Im Rahmen der Entwicklung gilt es, die Blockchain-Lösung an die technischen Anforderungen der

beteiligten Parteien anzupassen. Dies erfordert eine enge Abstimmung der jeweiligen IT-Abteilungen. Hier gilt es, durch technische Governance-Strukturen eine nachhaltig tragfähige Verteilung von Umsetzungskompetenzen und -verantwortungen zu definieren. Je nach gewünschter Ausgestaltung der Blockchain gilt es zudem, diese Verteilung in einem entsprechenden Entwicklungsmodell zu konkretisieren.

Im Rahmen der technischen Governance müssen zudem sowohl die Betriebsfragen zur Blockchain-Schicht selbst als auch zu den darunter liegenden Software- und Hardware-schichten adressiert werden. Grundsätzlich sollten diesbezügliche Entscheidungen den beteiligten Parteien selbst überlassen bleiben. Gleichzeitig ist eine Blockchain-Lösung allerdings nur so performant und sicher wie ihr schwächstes Glied. Daher sollte die Auswahl möglicher Betriebsmodelle und Betreiber an bestimmte Mindestanforderungen geknüpft werden.

Organisatorische Governance

Im Rahmen der organisatorischen Governance einer Blockchain-Lösung gilt es sicherzustellen, dass die grundsätzlichen und fachlichen Anforderungen der beteiligten Parteien verlässlich in die Entwicklung des Systems einfließen. Zu den grundsätzlichen Anforderungen gehört in der öffentlichen Verwaltung in Deutschland beispielsweise die Berücksichtigung des föderalen Rahmens.

Governance im Pilotprojekt

Für die Pilotierung der Blockchain-Lösung im Kontext der AnkER-Einrichtung Dresden wird aktuell eine Vereinbarung zur gemeinsamen Verantwortung für die Vorgaben der DSGVO zwischen dem Bundesamt und der LDS erarbeitet. Im Rahmen der Pilotierung wird die Blockchain-Lösung aus Gründen der Einfachheit durch einen gemeinsamen Anbieter entwickelt und bereitgestellt. Im späteren Realbetrieb können jedoch die verschiedenen Behörden auf unterschiedliche Anbieter zurückgreifen. Gleichzeitig sollen im weiteren Projektverlauf Mindestanforderungen für die Hinzunahme weiterer Betreiber erarbeitet werden. Auf der organisatorischen Seite sieht das Pilotprojekt sowohl für die grundsätzlichen als auch die konkreten fachlichen Anforderungen gemeinsame Abstimmungs- und Entscheidungsrunden vor.

4.4 Skalierbarkeit

Um die Komplexität zu minimieren, werden im Rahmen der Pilotierung ausschließlich zwei Behörden an die Blockchain-Lösung angeschlossen. Gleichzeitig wurde bei der Gestaltung der Lösungsansätze ein besonderer Fokus auf Skalierbarkeit und Ausweitung auf andere Behörden und Asylprozessvarianten gelegt.

Hierzu hat das Bundesamt intensiv die Entwicklung anderer Blockchain-Lösungen in Deutschland und Europa evaluiert. Ein besonders vielversprechender

Anknüpfungspunkt stellt die geplante „European Blockchain Services Infrastructure“ dar, deren Entwicklung seit 2018 von der „European Blockchain Partnership“ (EBP) aktiv vorangetrieben wird. Ziel dieser europäischen Initiative ist es, eine Blockchain-Infrastruktur für die öffentliche Verwaltung in Europa zu schaffen, auf der verschiedenste Dienste angeboten und verschiedenste Anwendungsfälle umgesetzt werden können. Gleichzeitig stellt die EBP aktuell noch keine Spezifikationen und Empfehlungen zur Verfügung. Die Blockchain-Lösung des Bundesamtes beruht entsprechend insbesondere auf Best Practices erfolgreicher Projekte aus der Industrie.

Konkret erstrecken sich diese Best Practices, ähnlich wie das Governance-Konzept, auf die Bereiche Datenschutz, Technik und organisatorische Ausgestaltung.

Datenschutzrechtliche Skalierbarkeit

Im Sinne der DSGVO muss stets eine einzelne verantwortliche Stelle für die Verarbeitung und Speicherung von Daten benannt werden. Alternativ kann diese Rolle auch von mehreren oder allen Stellen gemeinschaftlich (Joint Control) eingenommen werden. In diesem Fall ist eine Vereinbarung zu treffen, welche die Details der gemeinschaftlichen Verantwortung regelt.

Eine gemeinschaftliche Verantwortung durch alle Behörden kann im Realbetrieb mit einer Vielzahl

von Behörden nicht sinnvoll umgesetzt werden. Dennoch wird es vermutlich notwendig sein, dass ausgewählte Behörden (u.a. das Bundesamt) gemeinschaftlich die Verantwortung übernehmen. Die Vereinbarung zwischen dem Bundesamt und der LDS wird entsprechend rollenbasiert und erweiterbar gestaltet, um eine Hinzunahme weiterer Behörden in verschiedenen Rollen zu ermöglichen.

Technische Skalierbarkeit

Im Sinne der technischen Skalierbarkeit müssen weitere Behörden einfach angeschlossen werden können. Daher setzt die Blockchain-Lösung auf die Entwicklung einer Referenzarchitektur, welche aus Standardschnittstellen, gängige Technologien sowie einem flexibel erweiterbarem Datenmodell besteht. Die Verantwortung für die Integration der Blockchain-Lösung in das Bestandssystem liegt dabei bei der neu hinzukommenden Behörde. Jede Behörde kann selbst entscheiden, welche Daten und auf welche Weise sie diese Daten aus der Blockchain verarbeiten möchte (z.B. individuelle Warnfunktionen bei Prozessabweichungen). Dadurch bleibt die Komplexität der Blockchain – auch bei einer sehr großen Anzahl von Behörden handhabbar.

Zudem erlaubt die Blockchain-Lösung verschiedene Hosting-Ansätze und ermöglicht über Standardkonfigurationen auch Behörden ohne Blockchain-Vorwissen einen schnellen Anschluss.

Organisatorische Skalierbarkeit

Die organisatorische Skalierbarkeit umfasst zwei wesentliche Aspekte. Zum einen muss sichergestellt werden, dass auch die Anforderungen weiterer Behörden (z. B. Sicherheitsbehörden) umsetzbar sind. Zum anderen muss sichergestellt werden, dass neuen Behörden die Möglichkeit zur Mitgestaltung eingeräumt wird, ohne dass Entscheidungsprozesse substantiell an Agilität einbüßen.

Hier setzt das Bundesamt analog zur datenschutzrechtlichen Skalierbarkeit auf kleine Arbeitsgruppen, in denen ein Teil der beteiligten Behörden die Interessen des Netzwerks vertreten.

5. Design-Prinzipien für Blockchain-Lösungen in der öffentlichen Verwaltung

Im Rahmen der Konzeptionsphase hat das Bundesamt wichtige Grundlagenarbeit im Bereich datenschutzkonformer und anforderungsgerechter Gestaltung von Blockchain-Lösungen für die öffentliche Verwaltung geleistet. Dies war notwendig, da aktuell noch keine Best Practices oder Referenzimplementierungen für die deutsche Verwaltung existieren. Insbesondere fehlen aktuell Erfahrungswerte, inwiefern Blockchain-inhärente Eigenschaften, wie zum Beispiel die Nichtlöscharkeit, mit den Vorgaben der DSGVO in Einklang zu bringen sind.

Diese Erfahrungswerte und Erkenntnisse des Bundesamtes lassen sich in vier grundlegenden Design-Prinzipien zusammenfassen.

Design-Prinzip 1: Personenbezogene Daten sollen nicht auf der Blockchain gespeichert werden

Es soll vermieden werden, personenbezogene Daten auf der Blockchain zu speichern. Personenbezogene Daten sollten in den jeweiligen Bestandssystemen verbleiben.

Dieser Grundsatz sollte nach Einschätzung des Bundesamtes auch auf Hash-Werte personenbezogener Daten angewendet werden, da Fortschritte in der Rechenleistung letztendlich alte Hash-Funktionen mit vertretbarem Aufwand reversibel machen könnten.

Kritisch sind zudem konkrete Zuordnungsmerkmale auf der Blockchain. Sobald Daten auf der Blockchain alleinstehend zur Identifizierung einer natürlichen Person verwendet werden können, stellen diese personenbezogene Daten dar, die der DSGVO unterliegen. Entsprechend sollten die Daten in der Blockchain soweit wie möglich minimiert sowie von der Verwendung bestehender IDs auf der Blockchain abgesehen werden.

Design-Prinzip 2: Wenn ein Anwendungsfall erfordert, dass Daten in der Blockchain einer natürlichen Person zuordbar sind, soll eine hochsichere Off-Chain-Mapping-Architektur verwendet werden

Bestimmte Anwendungsfälle, wie die des Bundesamtes, erfordern, dass Informationen, die in der Blockchain gespeichert werden, bei Bedarf einem Asylgesuch bzw. einem Asylantrag zugeordnet werden können. Damit können die Informationen auch einer natürlichen Person, nämlich dem jeweiligen Asylsuchenden bzw. Asylantragstellenden zugeordnet werden. Da auch in diesen Anwendungsfällen das Design-Prinzip 1 gilt, dürfen die Informationen auf der Blockchain nicht so gestaltet sein, dass ohne zusätzliche Informationen auf eine natürliche Person geschlossen werden kann.

Daher sollte auf eine Pseudonymisierungslösung zurückgegriffen werden. Hier empfiehlt sich insbesondere der Einsatz von Mapping-Lösungen, welche pseudonyme Zuordnungsmerkmale auf der Blockchain mit dem von den jeweiligen Organisationen verwendeten konkreten Zuordnungsmerkmalen verknüpfen. Diese Mapping-Lösungen sollten off-chain gestaltet werden und Mapping-Informationen nur über sichere Informationskanäle austauschen.

Mit solchen Mapping-Lösungen können datenverantwortliche Stellen dem Recht auf Berechtigung und Löschung genügen, indem sie durch Korrekturtransaktionen „korrigieren“, und durch Löschung des Mappings die Daten auf der Blockchain aus ihrer subjektiven Perspektive entpersonalisieren, d.h. „löschen“.

Design-Prinzip 3: Blockchain soll als Komponente einer Gesamtlösung zur Verbesserung der Kommunikation und Zusammenarbeit betrachtet werden

Blockchain-Lösungen sollten nicht als losgelöste Systeme konzipiert werden. Stattdessen kann eine Blockchain-Lösung durch die Verteilung von Prozess-Updates an alle Mitglieder des Blockchain-Netzwerks eine Gesamtlösung zur Verbesserung der Kommunikation und Zusammenarbeit ermöglichen. Konkret kann eine Blockchain-Lösung sowohl pull- als auch push-basierten Austausch von Daten ermöglichen. Bei einem pull-basierten Austausch kann sich eine Behörde, wenn diese ein

relevantes Prozess-Update erkennt, für weitere Informationen an die ausstellende Behörde wenden. Die ausstellende Behörde kann dann jede dieser einzelnen Anfragen prüfen, dokumentieren und – falls unbegründet – ablehnen. Sie kann auf legitime Anfragen über sichere, Ende-zu-Ende-verschlüsselte und etablierte Informationskanäle reagieren. Bei einem push-basiertem Austausch hingegen, sendet die ausstellende Behörde entsprechend das Prozess-Update und gegebenenfalls die relevanten Informationen dazu an andere betroffene Behörden. Damit der Austausch unter den Behörden reibungslos funktioniert, müssen sich alle Behörden im Blockchain-Netzwerk auf Standards für den Datenaustausch einigen.

Design-Prinzip 4: Die Blockchain soll als getrennte, modulare Systemebene implementiert werden

Eine Blockchain sollte nicht genutzt werden, um Funktionen zu erfüllen, die von bewährten Lösungen wie zentralen Datenbanken besser bedient werden könnten. Blockchain ist keine gute Wahl, wenn eine Anwendung eine einzige, leicht zugängliche Datenbank für große Datenmengen benötigt, die in nahezu Echtzeit aktualisiert werden kann. Zudem ist es schwierig, Blockchain zur Unterstützung von Prozessen zu verwenden, die derzeit effektiver von etablierten Workflow-Management-Systemen unterstützt werden. Blockchain ist vielmehr eine Lösung für die Verteilung und Sicherung von Prozess-Updates zwischen Organisationen, wenn der Kontext

keine zentrale Steuerung des Workflows ermöglicht. Mit anderen Worten: Blockchain-Lösungen sollten eher eine ergänzende Rolle in einem kollaborativen organisationsübergreifendem Kontext spielen. Auf diese Weise ermöglicht Blockchain einen effektiveren Informationsaustausch zwischen fragmentierten Datenspeichern.

Zudem sollte das Design der Blockchain-Lösung lose gekoppelte Komponenten, standardisierte Schnittstellen sowie ein flexibel erweiterbares Datenmodell beinhalten. Diese Elemente ermöglichen die effiziente Wartung, Weiterentwicklung oder - falls erforderlich - den Austausch der Blockchain-Ebene zu einem späteren Zeitpunkt. Sie erzwingen auch die Abstraktion vom Blockchain-Protokoll und ermöglichen anderen Organisationen eine einfache Verbindung zum Blockchain-Netzwerk.

6. Ausblick

Aktuell befindet sich das Pilotprojekt in der Entwicklungsphase, die bis Ende des Jahres 2019 abgeschlossen werden soll. In dieser Phase werden die vorgestellten Konzepte umgesetzt. Hieran soll sich eine dreimonatige Erprobungs- und Evaluationsphase im beschränkten Wirkbetrieb Anfang nächsten Jahres anschließen.

Um die genauen Vorteile einer Blockchain-Lösung zu evaluieren, ist eine sach- und fachgerechte Untersuchung und Bewertung der Veränderungen im Asylprozess im Kontext der AnkER-Einrichtung Dresden geplant. Im Allgemeinen soll die Evaluation zeigen, ob und inwieweit die Blockchain-Technologie geeignet erscheint und den angestrebten Zweck erfüllt. Für die Evaluation sollen Daten methodisch erhoben, umfassend analysiert und systematisch dokumentiert werden, um die Untersuchung, das Vorgehen und die Ergebnisse nachvollziehbar und überprüfbar zu machen. Die Bewertung erfolgt dabei durch den Vergleich der ermittelten Werte vor (ex ante-Werte) und nach der Einführung (ex post-Werte) der Blockchain-Lösung.

Das Bundesamt verspricht sich ein deutliches Verbesserungspotential hinsichtlich Transparenz, Effizienz, Integrität und Kommunikation in der behördenübergreifenden Zusammenarbeit im Asylprozess in AnkER-Einrichtungen. Diese Vorteile würden deutlich mit jeder weiteren Behörde steigen, die an die Blockchain-Lösung angeschlossen werden kann. Zudem erwartet sich das Bundesamt aus der Pilotierung richtungsweisende Erkenntnisse und Erfahrungswerte zur dezentralen Gestaltung behör-

denübergreifender IT-Systeme. Derartige Systeme spiegeln die subsidiären und föderalen Organisationsstrukturen Deutschlands besser als zentrale Systeme wider und könnten damit einen grundlegenden Beitrag zur Digitalisierung und Vernetzung der Kommunal-, Landes- und Bundesbehörden leisten. Das Pilotprojekt nimmt daher eine Vorreiterrolle in Deutschland unter den laufenden IT-Projekten deutscher Bundesbehörden ein.

Im Falle einer positiven Pilotierung sind verschiedene Ausweitungsszenarien der Blockchain-Lösung denkbar. Zunächst könnten beispielsweise bestehende Prozessschritte des Asylprozesses in AnkER-Einrichtungen weiter untergliedert oder neue Prozessschritte (z.B. Widerrufs- und Rücknahmeverfahren) hinzugefügt werden. Neben der Hinzunahme von neuen Prozessschritten ist auch die Hinzunahme von weiteren Behörden im Asylprozess möglich. Hier sollte im ersten Schritt eine Ausweitung auf weitere AnkER-Einrichtungen oder funktionsgleiche Einrichtungen in Sachsen oder anderen Bundesländern angestrebt werden. Eine weitere Möglichkeit besteht darin, die Blockchain-Lösung auch für weitere Anwendungsfälle (z.B. Integrationsprozess) oder gar andere Kontexte zu nutzen. Hierbei können wiederum die ausgearbeiteten Konzepte und Design-Prinzipien als Grundlage und Richtlinie dienen.

Gleichzeitig sollte beachtet werden, dass andere Anwendungsfälle oder Kontexte auch andere Anforderungen an die Konzeption der Blockchain-Lösung stellen können, weshalb eine „One-fits-all“-Lösung

nicht empfehlenswert erscheint und gegebenenfalls Anpassungen vorgenommen werden müssen. Die daraus resultierenden verschiedenen Blockchain-Lösungen sollten allerdings miteinander kombinierbar sein, so dass eine Infrastruktur verschiedener Blockchain-Lösungen entstehen kann. Ausgehend von dieser Infrastruktur ist neben einer deutschlandweiten auch eine europaweite Lösung denkbar. Konkret könnten die Asylbehörden aller EU-Staaten zum Beispiel das Dublin-Verfahren wesentlich transparenter und effizienter über eine gemeinsame Blockchain-Infrastruktur abwickeln – ohne die Hoheit über nationale Daten an einen zentralen Server auf EU-Ebene abgeben zu müssen.

Aufgrund der föderalen Strukturen innerhalb Deutschlands und der Europäischen Union müsste eine solche Infrastruktur jedoch so ausgestaltet sein, dass sie die jeweiligen Strukturen und damit verbundenen Herausforderungen im Hinblick auf Zuständigkeiten, Prozessvarianten und die geltende Rechtslage abbilden kann. In diesem Sinne wäre Blockchain der „digitale Enabler“ des europäischen Föderalismus im Asylkontext und könnte gar ein weiterer Schritt hin zu einem gemeinsamen Europa sein.

7. Literaturverzeichnis

Androulaki, Elli; Manevich, Yacov; Muralidharan, Srinivasan; Murthy, Chet; Nguyen, Binh; Sethi, Manish 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.; Felten, Edward W. (2015): Sok. Research perspectives and challenges for bitcoin and cryptocurrencies. In: IEEE Symposium on Security and Privacy, S. 104–121.

Bundesamt für Migration und Flüchtlinge (2018): AnkER-Einrichtung – Ein Überblick. Online verfügbar unter http://www.bamf.de/SharedDocs/Anlagen/DE/Downloads/Infothek/DasBAMF/anker-einrichtungen-ueberblick.pdf?__blob=publicationFile, zuletzt geprüft am 11.04.2019.

Bundesamt für Migration und Flüchtlinge (2019): Ablauf des deutschen Asylverfahrens. Ein Überblick über die einzelnen Verfahrensschritte und rechtlichen Grundlagen. Unter Mitarbeit von Saliha Kubilay. Hg. v. Bundesamt für Migration und Flüchtlinge und Publikationsstelle des Bundesamtes für Migration und Flüchtlinge. Online verfügbar unter https://www.bamf.de/SharedDocs/Anlagen/DE/Publikationen/Broschueren/das-deutsche-asylverfahren.pdf?__blob=publicationFile, zuletzt geprüft am 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): Unterstützung der Kommunikation und Zusammenarbeit im Asylprozess mit Hilfe von Blockchain. Online verfügbar unter http://www.bamf.de/SharedDocs/Anlagen/DE/Downloads/Infothek/DasBAMF/blockchain-whitepaper.pdf?__blob=publicationFile, zuletzt geprüft am 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: Proceedings 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 Engineering (BISE) of the Fraunhofer Institute for Applied Information Technology FIT, Augsburg/Bayreuth. Online verfügbar unter https://www.fim-rc.de/wp-content/uploads/Fraunhofer-Studie_Digitale-Transformation.pdf, zuletzt geprüft am 11.04.2019.

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

Le Hors, Arnaud; Ferris, Christopher; Singh, Gari (2018): Hyperleder Fabric. Architecture Explained. Unter Mitarbeit von github.com. Hg. v. hyperledger-fabric.readthedocs.io. Online verfügbar unter <http://hyperledger-fabric.readthedocs.io/en/release-1.1/archdeep-dive.html>, zuletzt geprüft am 11.04.2019.

Linux Foundation (2017): Hyperledger Architecture Vol. I. Introduction to Hyperledger Business Blockchain Design Philosophy and Consensus. Unter Mitarbeit von 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. Online verfügbar unter https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf, zuletzt geprüft am 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. Online verfügbar unter <https://dl.eusset.eu/handle/20.500.12015/3161>, zuletzt geprüft am 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.): Proceedings of the 38th International Conference on Information Systems. Seoul, South Korea.

Disclaimer

Dieses White Paper wurde von der Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT nach bestem Wissen und unter Einhaltung der nötigen Sorgfalt erstellt.

Fraunhofer FIT, seine gesetzlichen Vertreter und/oder Erfüllungsgehilfen übernehmen keinerlei Garantie dafür, dass die Inhalte dieses White Papers gesichert, vollständig für bestimmte Zwecke brauchbar oder in sonstiger Weise frei von Fehlern sind. Die Nutzung dieses White Papers geschieht ausschließlich auf eigene Verantwortung.

In keinem Fall haften Fraunhofer FIT, seine gesetzlichen Vertreter und/oder Erfüllungsgehilfen für jegliche Schäden, seien sie mittelbar oder unmittelbar, die aus der Nutzung des White Papers resultieren.

Impressum

Herausgeber:

Bundesamt für Migration und Flüchtlinge
90461 Nürnberg

Redaktion:

Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT

Stand:

08/2019

Druck:

Bundesamt für Migration und Flüchtlinge, 90461 Nürnberg

Gestaltung:

DOK SYSTEME Ingenieurgesellschaft für Kommunikationstechnik mbH

Bildnachweis:

Titelbild: ©iStock matejmo; Abbildung 1: ©BAMF; Deutschlandkarte ©Shutterstock, Filip Bjorkman;
Alle übrigen Abbildungen: ©Fraunhofer FIT; ©DOK SYSTEME Ingenieurgesellschaft für
Kommunikationstechnik mbH

Empfohlene Zitierweise:

Fridgen, G., Guggenmos, F., Lockl, J., Rieger, A.; Urbach, N. und Wenninger, A. 2019. Entwicklung einer datenschutzkonformen Blockchain-Lösung im deutschen Asylprozess – Pilotierung im Kontext der AnKER-Einrichtung Dresden. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, Hrsg.: Bundesamt für Migration und Flüchtlinge (Nürnberg)

Bestellmöglichkeit:

Publikationsstelle des BAMF:
www.bamf.de/publikationen

Diese Publikation wird vom Bundesamt für Migration und Flüchtlinge im Rahmen seiner Öffentlichkeitsarbeit herausgegeben. Die Publikation wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.

Besuchen Sie uns auf:

www.facebook.com/bamf.socialmedia

@BAMF_Dialog

www.bamf.de/blockchain

